Full-duplex cyber-weapon with massive arrays

Nguyen, N-P., Ngo, H. Q., Duong, T. Q., Tuan, H. D., & da Costa, D. B. (2017). Full-duplex cyber-weapon with massive arrays. *IEEE Transactions on Communications*, *65*(12), 5544 - 5558. https://doi.org/10.1109/TCOMM.2017.2743208

Published in:
IEEE Transactions on Communications

Document Version:
Peer reviewed version

Full-Duplex Cyber-Weapon with Massive Arrays

Nam-Phong Nguyen, Hien Quoc Ngo, Trung Q. Duong, Hoang Duong Tuan, and Daniel B. da Costa

***Abstract*—In order to enhance secrecy performance of protecting scenarios, understanding the illegitimate side is crucial. In this paper, from the perspective of the illegitimate side, the security attack from a full-duplex cyber-weapon equipped with massive antenna arrays is considered. To evaluate the behavior of the proposed cyber-weapon, we develop a closed-form, a tight approximation, and asymptotic expressions of the achievable ergodic secrecy rate with taking into consideration imperfect channel estimation at the cyber-weapon. The results show that even under some disadvantage conditions, i.e., imperfect channel estimation and self-interference, the full-duplex massive array cyber-weapon can disable traditional physical layer protecting schemes, i.e., increasing the transmit power and the number of antennas at the legitimate transmitter. In addition, when a transmit power optimization scheme for maximizing the difference between the eavesdropping rate and the legitimate rate is applied at the full-duplex cyber-weapon, the malicious attack is even more dangerous. The results also reveal that when the legitimate side faces an advance adversary, it is essential to prevent important information in the training phases exposing to the illegitimate side.**

***Index Terms*—Physical layer security, full-duplex, massive MIMO, active eavesdropper, jamming, cyber-weapon.**

I. Introduction

Massive multiple-input multiple-output (MIMO) systems have become one of the key candidates for the next generation of wireless networks. In massive MIMO networks, the transmitters are equipped with a large number of antennas to serve end-users at the same time in the same frequency [1]. The advantage of massive MIMO is that the linear signal processing at the transmitter is nearly optimal thanks to the large number of antennas. Therefore, increasing the number of antennas at the transmitter can enhance the array gain with simple signal processing. Besides, the energy-efficiency and spectrum-efficiency of massive MIMO networks have been shown in [2].

Securing information is a challenge with the rapid development of wireless communication. Alongside with the conventional cryptography protocol, physical layer security (PLS) for wireless communication has attracted intensive attention from the research community recently [3]. The principle of PLS is to use the randomness of wireless channels to secure the transmission. By deploying PLS on top of the conventional cryptography protocols, the secrecy performance of wireless communication is enhanced [4]–[7]. There have been studies on PLS in massive MIMO networks. Artificial noise aided protecting schemes for massive MIMO networks under the malicious attack of multi-antenna passive eavesdropper were investigated in [8]. In [9], the secrecy performance of massive MIMO relay networks was studied. In [10], the authors proposed an uplink original symbol phase rotated scenario to protect the uplink transmission in a massive MIMO network in the presence of a massive MIMO eavesdropper. Power control schemes for training and data transmission to enhance the security of massive MIMO systems with the help of artificial noise were studied in [11]. In [12], the authors proposed various data precoders and artificial noise precoder to secure downlink transmission of a multi-cell massive MIMO system with large numbers of terminal users and antennas at the eavesdropper. The aforementioned works focused on designing the protecting schemes for the legitimate side and considered the passive eavesdroppers. However, the viewpoint of the illegitimate side is also important.

A. Related Works

Since understanding the abilities of the illegitimate side is also crucial to design effective protecting schemes for the legitimate side [13], [14]. This stream of research has attracted wide attention from the research community. In [15], an active half-duplex adversary that can perform as an eavesdropper or a jammer based on the legitimate side's strategy was studied. In [16], secure strategies of a multi-cell multi-user massive MIMO system under the malicious attempt of a multi-antenna active eavesdropper were proposed. In [17], the channel estimation and jamming process of a massive MIMO eavesdropper for attacking a time division duplex (TDD) system were demonstrated. In [18], the behavior of a wireless powered adversary that can operate randomly as a jammer or an eavesdropper was investigated. In addition, a power splitting and jamming/eavesdropping probability selection scheme based on the available power at the adversary were proposed. However, the adversaries in these works can perform only eavesdropping or jamming.

Yet, the introduction of full-duplex radio, which is promising to double the spectrum efficiency by allowing a wireless node to transmit and receive signals simultaneously in the same frequency band [19], has enabled the adversaries to perform eavesdropping and jamming at the same time. This topic has been investigated widely in the literature. In [20], an optimization scheme for a number of transmit and receive antennas at the full-duplex MIMO adversary was proposed

This paper has been submitted in part for presentation in IEEE GLOBECOM Workshop on Trusted Communications with Physical Layer Security, Singapore, December 2017.

This work was supported in part by the U.K. Royal Academy of Engineering Research Fellowship under Grant RF1415/14/22 and U.K. Engineering and Physical Sciences Research Council under Grant EP/P019374/1 and in part by the Australian Research Councils Discovery Projects under Project DP130104617.

N.-P. Nguyen, H. Q. Ngo, and T. Q. Duong are with Queen's University Belfast, U.K. (email: {pnguyen04, h.ngo, trung.q.duong}@qub.ac.uk).

H. D. Tuan is with University of Technology Sydney, Australia (e-mail: tuan.hoang@uts.edu.au).

D. B. da Costa is with University of Ceará, Brazil (email: danielbcosta@ieee.org).

in a multiple-input, multiple-output, multiple eavesdroppers (MIMOME) wiretap channel. A security scenario, in which a full-duplex eavesdropper attacks the training phase to modify the precoder at the transmitter, was presented in [21]. In [22], the authors proposed a rate maximization scheme for an active full-duplex legitimate monitor to efficiently eavesdrop a suspicious receiver with the assumption that the self-interference is perfectly cancelled. In [23], a full-duplex active eavesdropper equipped with one transmit and one receive antenna is considered. The optimization schemes for the performance of the legitimate and illegitimate side was formulated in a game frame work where the eavesdropper acts as the leader and the legitimate user is the follower. The case of partial channel state information is available at the legitimate users was also considered. The spoofing attack, in which the active adversary tries to modify the channel state information (CSI) of the legitimate channel to obtain more confidential information, was considered in [24].

However, to the best of the authors' knowledge, the malicious abilities of a powerful adversary, which is equipped with advanced technologies, i.e., full-duplex radio and massive array, have not been well-understood and considered in the literature. Motivated by the aforementioned discussions, in this paper, the abilities of a full-duplex massive array cyber-weapon in a conventional massive MISO system are investigated. In this scenario, the cyber-weapon is passive during the training phases to obtain CSI of the eavesdropping and jamming channels and then performs eavesdropping the confidential information and jamming the receiver simultaneously. Some related practical scenarios are: when the police and other first responder personnel want to interfere the private mobile radio systems and obtain important information; the thief wants to attack the wireless alarm systems in single-family homes so that the burglary will not be detected; or jamming against LTE, when used for private mobile radio applications.

B. Contributions

The contributions of this paper are summarized as follows:

- In order to study the behavior of the proposed cyber-weapon, we derive exact closed-form expressions and tight approximations of the achievable ergodic secrecy rate of the considered system in the perfect and imperfect channel estimation scenarios at the cyber-weapon.
- We demonstrate that increasing the number of receive antennas at the adversary can reduce the effect of the self-interference imposed by full-duplex mechanism. In addition, increasing the number of transmit antennas, i.e., N, at the adversary can reduce the jamming power proportionally to $\frac{1}{N^\alpha}$, $0 < \alpha < 1$. It is proved that with a certain proportion of the number of antennas at the adversary to the number of antennas at the information source, the illegitimate side can guarantee a zero secrecy rate. Besides, the illegitimate side benefits from increasing the transmit power at the legitimate side. Therefore, using high transmit power at the legitimate side does not guarantee an enhancement in the secrecy performance.

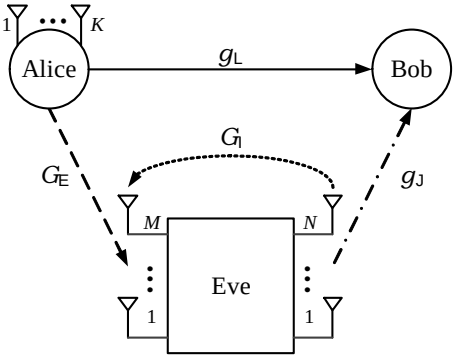

Fig. 1: System model.

- A power optimization scheme at the adversary to maximize the difference between the eavesdropping rate and the legitimate rate is proposed. The result shows that by applying the power optimization scheme, the adversary can launch the malicious attack more effectively.

The rest of this paper is organized as follows. The system and channel models are described in Section II. The exact closed-form, approximating, and asymptotic expressions of the system's achievable ergodic secrecy rate in the perfect channel estimation at the cyber-weapon are presented in Section III. In Section IV, a specific channel estimation scheme at the cyber-weapon is proposed and evaluated. The numerical results based on Monte-Carlo methods are presented in Section V to confirm the tightness of the approximations and the correctness of our analyses. Finally, we conclude this paper in Section VI.

II. System and Channel Models

In this paper, we consider a malicious attack in which a cyber-weapon Eve tries to jam the legitimate receiver Bob and eavesdrop the confidential informational from the legitimate transmitter Alice simultaneously. In the considered system, Alice is equipped with K antennas and Bob is equipped with a single antenna [1]. Meanwhile, Eve operates in full-duplex mode and is equipped with M receive antennas and N transmit antennas.

In this system, Alice transmits confidential messages to Bob over channel vector $\boldsymbol{g}_{\mathsf{L}}$ which is modeled by the independent small-scale fading and large-scale fading (geometric attenuation and shadow fading). The channel vector $\boldsymbol{g}_{\mathsf{L}}$ is expressed as

$$\boldsymbol{g}_{\mathsf{L}} = \sqrt{\beta_{\mathsf{L}}}\boldsymbol{h}_{\mathsf{L}}, \tag{1}$$

[1]The assumption of a single-antenna at users in massive MIMO system are widely deployed in the literature because of its cost-efficiency, power efficiency, simplicity, and typically high throughput [13], [16], [25]. In addition, the case of one single-antenna users can be considered as a special case of multi-antennas users when the auxiliary antennas can be treated as additional users. Under the assumption on favorable propagation in massive MIMO, which holds true when the number of antennas at the transmitter is large, k autonomous single-antenna users system and one k-antenna user system have the same energy and spectral efficiency [25]. Besides, the assumption of a single antenna at Bob makes the considered system simple to analyze that provides important insights. Particularly, in the case of multiple antennas are deployed at Bob, the secrecy rate of the considered system still goes to zero when the numbers of antennas at Alice and Eve go to infinity. The detailed proof is provided in Appendix E.

where $\boldsymbol{h}_{\mathsf{L}}$ is the $K \times 1$ small-scale fading vector, $\boldsymbol{h}_{\mathsf{L}} \sim \mathcal{CN}(0, \boldsymbol{I}_K)$, and β_{L} is the large-scale fading coefficient of the legitimate channel. At the same time, Eve wiretaps these confidential messages at her receive antennas over $K \times M$ channel matrix $\boldsymbol{G}_{\mathsf{E}}$ which can be written as

$$\boldsymbol{G}_{\mathsf{E}} = \sqrt{\beta_{\mathsf{E}}}\boldsymbol{H}_{\mathsf{E}}, \tag{2}$$

where $\boldsymbol{H}_{\mathsf{E}}$ is the matrix of small-scale fading coefficients whose elements are $\mathcal{CN}(0,1)$ independent and identically distributed (i.i.d.), and β_{E} is the large-scale fading coefficient of the eavesdropping channel. Meanwhile, at the transmit antennas of Eve, jamming signals are transmitted to Bob to confuse the decoding process. The channel between Eve and Bob is modeled as follows:

$$\boldsymbol{g}_{\mathsf{J}} = \sqrt{\beta_{\mathsf{J}}}\boldsymbol{h}_{\mathsf{J}}, \tag{3}$$

where $\boldsymbol{h}_{\mathsf{J}} \sim \mathcal{CN}(0, \boldsymbol{I}_N)$ is the $N \times 1$ vector of small-scale fading coefficients and β_{J} is the large-scale fading coefficient of the jamming channel.

In receiving and transmitting signals simultaneously, Eve suffers from self-interference. The self-interference between the transmit and receive antennas of Eve is modeled as an $M \times N$ channel matrix

$$\boldsymbol{G}_{\mathsf{I}} = \sigma_{\mathsf{I}}\boldsymbol{H}_{\mathsf{I}}, \tag{4}$$

whose elements are $\mathcal{CN}(0,1)$ i.i.d., and σ_{I} represents the normalized self-interference impact. If $\sigma_{\mathsf{I}} = 0$, the self-interference is perfectly cancelled out. Evaluating sef-interference cancellation/isolation techniques is out of the scope of this paper.

In this work, we consider a downlink communication of a TDD MISO system. During each coherence interval, there are three phases. In the first phase, Bob needs to transmit his pilot signals to Alice so that she can estimate the legitimate CSI for performing beamforming. In the second phase, Alice needs to beamform the downlink pilot to Bob so that he can estimate the effective channel gain which is used for signal detection [26], [27]. Finally, in the last phase, Alice transmits information to Bob. During the first two phases, Eve can take advantage of the pilots sent from Alice and Bob to estimate the eavesdropping and jamming channels. To emphasize our idea of a powerful adversary, we assume that the CSI of the legitimate channel is perfectly known at Alice [2]. Since Alice does not have the knowledge of CSI of the eavesdropping channel, she deploys maximal-ratio transmission (MRT)[3] which is an optimal linear precoder in multiple-input single-output (MISO) channels to transmit her signal to Bob [4]. With MRT, the transmit signal from Alice is formulated as

$$s = \sqrt{\mathcal{P}_{\mathsf{A}}}\frac{\boldsymbol{g}_{\mathsf{L}}}{\|\boldsymbol{g}_{\mathsf{L}}\|}x, \tag{5}$$

where $\|\cdot\|$ indicates the Frobenius norm, $\sqrt{\mathcal{P}_{\mathsf{A}}}\frac{\boldsymbol{g}_{\mathsf{L}}}{\|\boldsymbol{g}_{\mathsf{L}}\|}$ is the MRT pre-coding vector, x is the confidential message with $\mathbb{E}\left\{|x|^2\right\} = 1$, and $\mathcal{P}_{\mathsf{A}}$ is the average transmit power, i.e., $\mathbb{E}\left\{|s|^2\right\} = \mathcal{P}_{\mathsf{A}}$.

III. Perfect Channel Estimation at Eve

In this section, an assumption of perfect channel estimation at Eve is considered to provide a benchmark and initial insights of the considered system. The imperfect channel estimation scheme is discussed in detail in Section IV with a specific channel estimation method.

It is assumed that Eve can obtain perfect CSI of the eavesdropping and jamming links, i.e., it knows $\bar{\boldsymbol{g}}_{\mathsf{E}} = \boldsymbol{G}_{\mathsf{E}}^H\frac{\boldsymbol{g}_{\mathsf{L}}}{\|\boldsymbol{g}_{\mathsf{L}}\|}$ and $\boldsymbol{g}_{\mathsf{J}}$. This worst-case assumption is reasonable because Eve can take advantage of the pilots sent by Alice and Bob during the legitimate CSI exchanging phases for estimating $\bar{\boldsymbol{g}}_{\mathsf{E}}$ and $\boldsymbol{g}_{\mathsf{J}}$ [17].

The jamming signal from Eve is formulated as

$$s_{\mathsf{J}} = \sqrt{\mathcal{P}_{\mathsf{J}}}\frac{\boldsymbol{g}_{\mathsf{J}}}{\|\boldsymbol{g}_{\mathsf{J}}\|}x_{\mathsf{J}}, \tag{6}$$

where $\mathbb{E}\left\{|x_{\mathsf{J}}|^2\right\} = 1$ and $\mathcal{P}_{\mathsf{J}}$ is the average transmit power of Eve. As a consequence, the received signal at Bob is

$$\begin{aligned} y_{\mathsf{L}} &= \sqrt{\mathcal{P}_{\mathsf{A}}}\boldsymbol{g}_{\mathsf{L}}^H\frac{\boldsymbol{g}_{\mathsf{L}}}{\|\boldsymbol{g}_{\mathsf{L}}\|}x + \sqrt{\mathcal{P}_{\mathsf{J}}}\boldsymbol{g}_{\mathsf{J}}^H\frac{\boldsymbol{g}_{\mathsf{J}}}{\|\boldsymbol{g}_{\mathsf{J}}\|}x_{\mathsf{J}} + w_{\mathsf{L}} \\ &= \sqrt{\mathcal{P}_{\mathsf{A}}}\,\|\boldsymbol{g}_{\mathsf{L}}\|\,x + \sqrt{\mathcal{P}_{\mathsf{J}}}\,\|\boldsymbol{g}_{\mathsf{J}}\|\,x_{\mathsf{J}} + w_{\mathsf{L}}, \end{aligned} \tag{7}$$

where $w_{\mathsf{L}} \sim \mathcal{CN}(0, \sigma_0^2)$ is the additive white Gaussian noise (AWGN) at Bob.

Under the full-duplex mechanism, Eve receives both the confidential message and her self-interference. Therefore, the received signal at Eve is given as

$$\boldsymbol{y}_{\mathsf{E}} = \sqrt{\mathcal{P}_{\mathsf{A}}}\boldsymbol{G}_{\mathsf{E}}^H\frac{\boldsymbol{g}_{\mathsf{L}}}{\|\boldsymbol{g}_{\mathsf{L}}\|}x + \sqrt{\mathcal{P}_{\mathsf{J}}}\boldsymbol{G}_{\mathsf{I}}\frac{\boldsymbol{g}_{\mathsf{J}}}{\|\boldsymbol{g}_{\mathsf{J}}\|}x_{\mathsf{J}} + \boldsymbol{w}_{\mathsf{E}}, \tag{8}$$

where $\boldsymbol{w}_{\mathsf{E}} \sim \sigma_0\mathcal{CN}(0, \boldsymbol{I}_M)$ is the $M \times 1$ AWGN vector at the receiving side of Eve. Consequently, Eve uses $\bar{\boldsymbol{g}}_{\mathsf{E}}$ to perform maximal ratio combining (MRC). The MRC processed signal at Eve is

$$y_{\mathsf{E}}^{\mathsf{MRC}} = \frac{\bar{\boldsymbol{g}}_{\mathsf{E}}^H}{\|\bar{\boldsymbol{g}}_{\mathsf{E}}\|}\boldsymbol{y}_{\mathsf{E}} = \sqrt{\mathcal{P}_{\mathsf{A}}}\,\|\bar{\boldsymbol{g}}_{\mathsf{E}}\|\,x + \sqrt{\mathcal{P}_{\mathsf{J}}}\frac{\bar{\boldsymbol{g}}_{\mathsf{E}}^H}{\|\bar{\boldsymbol{g}}_{\mathsf{E}}\|}\bar{\boldsymbol{g}}_{\mathsf{I}}x_{\mathsf{J}} + \frac{\bar{\boldsymbol{g}}_{\mathsf{E}}^H}{\|\bar{\boldsymbol{g}}_{\mathsf{E}}\|}\boldsymbol{w}_{\mathsf{E}}, \tag{9}$$

where $\bar{\boldsymbol{g}}_{\mathsf{E}} = \boldsymbol{G}_{\mathsf{E}}^H\frac{\boldsymbol{g}_{\mathsf{L}}}{\|\boldsymbol{g}_{\mathsf{L}}\|}$ and $\bar{\boldsymbol{g}}_{\mathsf{I}} = \boldsymbol{G}_{\mathsf{I}}\frac{\boldsymbol{g}_{\mathsf{J}}}{\|\boldsymbol{g}_{\mathsf{J}}\|}$.

[2]Interested reader may find analysis and numerical results for the case of imperfect channel estimation at legitimate users in Appendix F.

[3]In the conventional massive MIMO/MISO networks, MRT is well-known for its good performance, low-complexity, and high cost-efficiency compared with the other two famous precoders, i.e., zero-forcing (ZF) and minimum mean-square error (MMSE) precoders which require huge amount of computational resources at the massive array transmitter. Besides, without any necessary knowledge of the adversary, it is hard for the legitimate side to design any enhancing secrecy performance precoders.

[4]In the conventional massive MIMO/MISO networks, using artificial noise (AN) can enhance the secrecy performance. However, without knowledge of the adversary, the conventional users have to use AN all the time which leads to inefficiency in using resources. This work aims to analyze and reveal some insights of a powerful adversary with advance technologies, i.e., massive arrays antennas and full-duplex radio. We let adequately protecting schemes for this kind of cyber-weapon for future work.

A. Closed-form Expressions for Finite K, M, N

1) Ergodic Legitimate Rate: Since Bob only knows the legitimate channel $\boldsymbol{g}_{\mathsf{L}}$, from (7), the ergodic legitimate rate is given as [5]

$$R_{\mathsf{L}} = \mathbb{E}_{\boldsymbol{g}_{\mathsf{L}}}\left\{\log_2\left(1+\frac{\mathbb{E}\left\{|\sqrt{\mathcal{P}_{\mathsf{A}}}\,\|\boldsymbol{g}_{\mathsf{L}}\|\,x|^2|\boldsymbol{g}_{\mathsf{L}}\right\}}{\mathbb{E}\left\{|\sqrt{\mathcal{P}_{\mathsf{J}}}\,\|\boldsymbol{g}_{\mathsf{J}}\|\,x_{\mathsf{J}}+\boldsymbol{w}_{\mathsf{E}}|^2|\boldsymbol{g}_{\mathsf{L}}\right\}}\right)\right\} = \mathbb{E}_{\boldsymbol{g}_{\mathsf{L}}}\left\{\log_2\left(1+\frac{\gamma_{\mathsf{A}}\,\|\boldsymbol{g}_{\mathsf{L}}\|^2}{\gamma_{\mathsf{J}}N\beta_{\mathsf{J}}+1}\right)\right\}, \tag{10}$$

where $\mathbb{E}\{X|Y\}$ is conditional expectation of X on Y, $\gamma_{\mathsf{A}} = \frac{\mathcal{P}_{\mathsf{A}}}{\sigma_0^2}$ and $\gamma_{\mathsf{J}} = \frac{\mathcal{P}_{\mathsf{J}}}{\sigma_0^2}$.

From (10), we have the following lemma

Lemma 1: The exact closed-form of the ergodic rate of the legitimate channel can be formulated as follows:

$$R_{\mathsf{L}} = \frac{1}{\ln 2}\sum_{k=0}^{K-1}\frac{1}{(K-1-k)!}\left(\frac{-\gamma_{\mathsf{J}}N\beta_{\mathsf{J}}-1}{\gamma_{\mathsf{A}}\beta_{\mathsf{L}}}\right)^{K-k-1} \times\left[-\exp\left(\frac{\gamma_{\mathsf{J}}N\beta_{\mathsf{J}}+1}{\gamma_{\mathsf{A}}\beta_{\mathsf{L}}}\right)\mathrm{Ei}\left(\frac{-\gamma_{\mathsf{J}}N\beta_{\mathsf{J}}-1}{\gamma_{\mathsf{A}}\beta_{\mathsf{L}}}\right) + \sum_{l=1}^{K-k-1}(l-1)!\left(\frac{-\gamma_{\mathsf{J}}N\beta_{\mathsf{J}}-1}{\gamma_{\mathsf{A}}\beta_{\mathsf{L}}}\right)^{-l}\right], \tag{11}$$

where $\mathrm{Ei}(\cdot)$ is the exponential integral function [28, Eq. (8.211.1)].

Proof: The proof is given in Appendix A. ∎

The closed-form expression (11) gives us some insights regarding the effects of K, N, γ_{J}, γ_{A}, and can be more efficiently evaluated compared with (10). However, it involves the complicated exponential integral function which is not easy to use for further designs of the considered system. Based (10), we have the following result.

Lemma 2: The ergodic rate of the legitimate channel is approximated as

$$R_{\mathsf{L}} \approx R_{\mathsf{L}}^{\mathsf{a}} \triangleq \log_2\left(1+\frac{\gamma_{\mathsf{A}}K\beta_{\mathsf{L}}}{\gamma_{\mathsf{J}}N\beta_{\mathsf{J}}+1}\right), \tag{12}$$

Proof: Eq. (12) is attained by using the identity

$$\frac{1}{M}\|\boldsymbol{v}\|^2 \overset{M\to\infty}{\to} \frac{1}{M}\mathbb{E}\left\{\|\boldsymbol{v}\|^2\right\} \tag{13}$$

where $\boldsymbol{v}\sim\mathcal{CN}(0,\boldsymbol{I}_M)$. ∎

2) Ergodic Eavesdropping Rate: From (9), applying the properties of circularly symmetric normal vectors, it is observed that

$$\bar{\boldsymbol{g}}_{\mathsf{I}} = \boldsymbol{G}_{\mathsf{I}}\frac{\boldsymbol{g}_{\mathsf{J}}}{\|\boldsymbol{g}_{\mathsf{J}}\|} \sim \sigma_{\mathsf{I}}\,\mathcal{CN}(0,\boldsymbol{I}_M) \tag{14}$$

and is independent of $\boldsymbol{g}_{\mathsf{J}}$. Similarly, $\frac{\bar{\boldsymbol{g}}_{\mathsf{E}}^H}{\|\bar{\boldsymbol{g}}_{\mathsf{E}}\|}\bar{\boldsymbol{g}}_{\mathsf{I}} \sim \mathcal{CN}(0,\sigma_{\mathsf{I}}^2)$, $\frac{\bar{\boldsymbol{g}}_{\mathsf{E}}^H}{\|\bar{\boldsymbol{g}}_{\mathsf{E}}\|}\boldsymbol{w}_{\mathsf{E}} \sim \mathcal{CN}(0,\sigma_0^2)$, and they are independent of $\bar{\boldsymbol{g}}_{\mathsf{E}}$. At Eve, the information of $\bar{\boldsymbol{g}}_{\mathsf{E}}$ and $\boldsymbol{g}_{\mathsf{J}}$ is available. Therefore, from (9), the ergodic rate of the eavesdropping channel is given as (15) on the top of the next page.

[5]This ergodic legitimate rate is obtained under the assumption of worst-case scenario where the interference plus noise is Gaussian distributed. This assumption is reasonable since the interference plus noise of (7) approximates to a Gaussian when the number of antennas at Eve is large.

Lemma 3: The ergodic rate of the eavesdropping channel admits the following closed-form:

$$R_{\mathsf{E}} = \frac{1}{\ln 2}\sum_{m=0}^{M-1}\frac{1}{(M-1-m)!}\left(\frac{-\gamma_{\mathsf{J}}\sigma_{\mathsf{I}}^2-1}{\gamma_{\mathsf{A}}\beta_{\mathsf{E}}}\right)^{M-m-1} \times\left[-\exp\left(\frac{\gamma_{\mathsf{J}}\sigma_{\mathsf{I}}^2+1}{\gamma_{\mathsf{A}}\beta_{\mathsf{E}}}\right)\mathrm{Ei}\left(\frac{-\gamma_{\mathsf{J}}\sigma_{\mathsf{I}}^2-1}{\gamma_{\mathsf{A}}\beta_{\mathsf{E}}}\right) + \sum_{p=1}^{M-m-1}(p-1)!\left(\frac{-\gamma_{\mathsf{J}}\sigma_{\mathsf{I}}^2-1}{\gamma_{\mathsf{A}}\beta_{\mathsf{E}}}\right)^{-p}\right]. \tag{16}$$

Proof: The proof is given in Appendix A. ∎

Remark 1: From (16), although Eve suffers from her self-interference, the ergodic eavesdropping rate does not depend on the number of transmit antennas at Eve. In addition, Eve can improve the ergodic eavesdropping rate by increasing her number of receive antennas.

The following lemma follows from (15).

Lemma 4: The eavesdropping channel's ergodic rate is approximated as

$$R_{\mathsf{E}} \approx R_{\mathsf{E}}^{\mathsf{a}} \triangleq \log_2\left(1+\frac{\gamma_{\mathsf{A}}M\beta_{\mathsf{E}}}{\gamma_{\mathsf{J}}\sigma_{\mathsf{I}}^2+1}\right). \tag{17}$$

Proof: Eq. (17) is obtained by using the identity (13). ∎

3) Achievable Ergodic Secrecy Rate: From (11) and (16), the following theorem is given.

Theorem 1: The exact-closed form expression of the achievable ergodic secrecy rate is given as

$$R_{\mathsf{S}} \triangleq [R_{\mathsf{L}} - R_{\mathsf{E}}]^+, \tag{18}$$

where R_{L} and R_{E} are given in (11) and (16), respectively, and $[x]^+ = \max(x,0)$.

Since this exact-closed form expression is complex, we develop an approximation of the achievable ergodic secrecy rate for further important insights, which is based on (12) and (17).

Theorem 2: The achievable ergodic secrecy rate is approximated as

$$R_{\mathsf{S}}^{\mathsf{a}} \triangleq [R_{\mathsf{L}}^{\mathsf{a}} - R_{\mathsf{E}}^{\mathsf{a}}]^+ = [\log_2(\Psi)]^+, \tag{19}$$

where

$$\Psi = 1+\frac{\gamma_{\mathsf{J}}\gamma_{\mathsf{A}}[K\beta_{\mathsf{L}}\sigma_{\mathsf{I}}^2 - M\beta_{\mathsf{E}}N\beta_{\mathsf{J}}] + \gamma_{\mathsf{A}}[K\beta_{\mathsf{L}} - M\beta_{\mathsf{E}}]}{(\gamma_{\mathsf{J}}\sigma_{\mathsf{I}}^2+1+\gamma_{\mathsf{A}}M\beta_{\mathsf{E}})(\gamma_{\mathsf{J}}N\beta_{\mathsf{J}}+1)}. \tag{20}$$

Typically, Alice tries to increase her transmit power to enhance the secrecy rate. From (19), to gain important insights of the considered system when the transmit power of Alice is high, we derive an asymptotic expression for the achievable ergodic secrecy rate.

Lemma 5: The asymptotic expression for the ergodic secrecy rate when the transmit power of Alice is high can be expressed as

$$R_{\mathsf{S}}^{\mathsf{u,asym}} \overset{\gamma_{\mathsf{A}}\to\infty}{\to} \left[\log_2\left(\frac{(\gamma_{\mathsf{J}}\sigma_{\mathsf{I}}^2+1)\beta_{\mathsf{L}}K}{(\gamma_{\mathsf{J}}N\beta_{\mathsf{J}}+1)M\beta_{\mathsf{E}}}\right)\right]^+. \tag{21}$$

Proof: The proof is given in Appendix B. ∎

From (21), we can observe that (i) increasing transmit power at Alice does not guarantee an improvement in the secrecy

$$R_{\mathsf{E}} = \mathbb{E}_{\bar{\boldsymbol{g}}_{\mathsf{E}},\boldsymbol{g}_{\mathsf{J}}}\left\{\log_2\left(1+\frac{\mathbb{E}\left\{|\sqrt{\mathcal{P}_{\mathsf{A}}}\,\|\bar{\boldsymbol{g}}_{\mathsf{E}}\|\,x|^2|\bar{\boldsymbol{g}}_{\mathsf{E}},\boldsymbol{g}_{\mathsf{J}}\right\}}{\mathbb{E}\left\{|\sqrt{\mathcal{P}_{\mathsf{J}}}\frac{\bar{\boldsymbol{g}}_{\mathsf{E}}^H}{\|\bar{\boldsymbol{g}}_{\mathsf{E}}\|}\bar{\boldsymbol{g}}_{\mathsf{I}}x_{\mathsf{J}}+\frac{\bar{\boldsymbol{g}}_{\mathsf{E}}^H}{\|\bar{\boldsymbol{g}}_{\mathsf{E}}\|}\boldsymbol{w}_{\mathsf{E}}|^2|\bar{\boldsymbol{g}}_{\mathsf{E}},\boldsymbol{g}_{\mathsf{J}}\right\}}\right)\right\} = \mathbb{E}_{\bar{\boldsymbol{g}}_{\mathsf{E}}}\left\{\log_2\left(1+\frac{\gamma_{\mathsf{A}}\,\|\bar{\boldsymbol{g}}_{\mathsf{E}}\|^2}{\gamma_{\mathsf{J}}\sigma_{\mathsf{I}}^2+1}\right)\right\}. \tag{15}$$

performance of the legitimate side, and (ii) the cyber-weapon can increase the numbers of its transmit and receive antennas to reduce the effect of self-interference and enhance the malicious attack.

B. Asymptotic Analysis

1) Power Scale Law at Eve: Eve can benefit a reduction in her transmit power by deploying a large number of transmit antennas.

Corollary 1: The transmit power at Eve can be reduced proportionally to $\left(\frac{1}{N}\right)^{\mu}$, where $0<\mu<1$.

Proof:

Plugging $\gamma_{\mathsf{J}} = \frac{\bar{\gamma}_{\mathsf{J}}}{N^{\mu}}$ into (19), where $\bar{\gamma}_{\mathsf{J}}$ is the maximal transmit power of Eve. When the number of transmit antennas at Eve is large, R_s can be rewritten as

$$R_{\mathsf{S}}^{\mathsf{a}} \overset{N\to\infty}{\to} \left[\log_2\left(\frac{1}{\gamma_{\mathsf{A}}\beta_{\mathsf{E}}M+1}\right)\right]^+ = 0. \tag{22}$$

■

Remark 2: From (22), increasing the number of transmit antennas at Eve can reduce the effect of the self-interference on the secrecy rate.

2) Rule of the Numbers of Antennas at Eve: It is popular to assume that Alice can increase the transmit power while Eve keeps the transmit power constant. However, Eve can also increase her power proportionally to Alice's transmit power for disturbing the legitimate channel. Therefore, when transmit power at Alice and Eve is high, an interesting question is that how many antennas Eve should deploy to guarantee $R_{\mathsf{S}}=0$. To answer this question, it is considered that the numbers of transmit and receive antennas at Eve are proportional to the number of transmit antennas at Alice, i.e., $N=\epsilon_n K^{\alpha}$, $M=\epsilon_m K^{\nu}$, and the transmit power at Eve is proportional to the transmit power at Alice, i.e., $\gamma_{\mathsf{J}}=\varrho\gamma_{\mathsf{A}}$, where $\epsilon_m>0$, $\epsilon_n>0$, $\alpha>0$, $\nu>0$, and $\varrho>0$. From (19), we have

$$R_{\mathsf{S}} = \left[\log_2\left(1+\frac{\varrho\gamma_{\mathsf{A}}^2[K\beta_{\mathsf{L}}\sigma_{\mathsf{I}}^2-\epsilon_n\epsilon_m K^{\nu+\alpha}\beta_{\mathsf{E}}\beta_{\mathsf{J}}]}{(\gamma_{\mathsf{A}}\varrho\sigma_{\mathsf{I}}^2+1+\gamma_{\mathsf{A}}K^{\nu}\beta_{\mathsf{E}})(\gamma_{\mathsf{A}}\varrho K^{\alpha}\beta_{\mathsf{J}}+1)}\right.\right.$$
$$\left.\left.+\frac{\gamma_{\mathsf{A}}[K\beta_{\mathsf{L}}-\epsilon_m K^{\nu}\beta_{\mathsf{E}}]}{(\gamma_{\mathsf{A}}\varrho\sigma_{\mathsf{I}}^2+1+\gamma_{\mathsf{A}}K^{\nu}\beta_{\mathsf{E}})(\gamma_{\mathsf{A}}\varrho K^{\alpha}\beta_{\mathsf{J}}+1)}\right)\right]^+. \tag{23}$$

When γ_{A} is high, R_s can be rewritten as follows:

$$R_{\mathsf{S}} \overset{\gamma_{\mathsf{A}}\to\infty}{\to} \left[\log_2\left(1+\frac{\varrho[K\beta_{\mathsf{L}}\sigma_{\mathsf{I}}^2-\epsilon_n\epsilon_m K^{\nu+\alpha}\beta_{\mathsf{E}}\beta_{\mathsf{J}}]}{\varrho\epsilon_n K^{\alpha}\beta_{\mathsf{J}}(\varrho\sigma_{\mathsf{I}}^2+\epsilon_m K^{\nu}\beta_{\mathsf{E}})}\right)\right]^+. \tag{24}$$

From (24), we have the following corollary.

Corollary 2: The number of antennas at Eve for keeping $R_{\mathsf{S}}=0$ must be chosen to satisfy the following condition.

$$\nu+\alpha > 1-\frac{\log\left(\frac{\epsilon_n\epsilon_m\beta_{\mathsf{E}}\beta_{\mathsf{J}}}{\beta_{\mathsf{L}}\sigma_{\mathsf{I}}^2}\right)}{\log(K)}. \tag{25}$$

Remark 3: From (25), the sum of the order of the transmit and receive antennas at Eve increases with logarithm function of the self-interference effect and it reduces when the number of transmit antennas at Alice increases.

C. Transmit Power Optimization Scheme for Cyber-weapon

From (19), we can observe that if the cyber-weapon increases transmit power for jamming process, the ergodic rate of legitimate link and eavesdropping link will reduce. The reason is that when the transmit power of jamming signal increases, the self-interference of full-duplex mechanism also increases at the receive antennas of Eve. However, reducing the transmit power of Eve will also reduce the ability of degrading legitimate channel. Therefore, to enhance the malicious attack, the transmit power at Eve should be optimized to maximize the difference between the eavesdropping rate and the legitimate rate. The optimization problem can be formulated as

$$\max_{\gamma_{\mathsf{J}}} \quad R_{\mathsf{E}}^{\mathsf{a}} - R_{\mathsf{L}}^{\mathsf{a}}$$
$$\text{s. t.} \quad R_{\mathsf{E}}^{\mathsf{a}} > R_{\mathsf{L}}^{\mathsf{a}}, \tag{26}$$
$$0 \le \gamma_{\mathsf{J}} \le \gamma_{\mathsf{Jmax}}, \tag{27}$$

where γ_{Jmax} is the maximal transmit power of Eve. From (26), an equivalent optimization problem can be expressed as

$$\max_{\gamma_{\mathsf{J}}} \quad \Theta(\gamma_{\mathsf{J}})$$
$$\text{s. t.} \quad a\gamma_{\mathsf{J}}+b>0, \tag{28}$$
$$0 \le \gamma_{\mathsf{J}} \le \gamma_{\mathsf{Jmax}}, \tag{29}$$

where $\Theta(\gamma_{\mathsf{J}}) = 1+\frac{a\gamma_{\mathsf{J}}+b}{c\gamma_{\mathsf{J}}^2+d\gamma_{\mathsf{J}}+e}$, $a=\gamma_{\mathsf{A}}[MN\beta_{\mathsf{J}}\beta_{\mathsf{E}}-\sigma_{\mathsf{I}}^2\beta_{\mathsf{L}}K]$, $b=\gamma_{\mathsf{A}}[M\beta_{\mathsf{E}}-K\beta_{\mathsf{L}}]$, $c=\sigma_{\mathsf{I}}^2N\beta_{\mathsf{J}}$, $d=\sigma_{\mathsf{I}}^2+\beta_{\mathsf{J}}N+\gamma_{\mathsf{A}}K\beta_{\mathsf{L}}\sigma_{\mathsf{I}}^2$, $e=1+\gamma_{\mathsf{A}}K\beta_{\mathsf{L}}$.

The optimal solution for transmit power γ_{J}^* is as follows:

$$\gamma_{\mathsf{J}}^* = \begin{cases} \arg\max\limits_{\gamma_{\mathsf{J}}\in\{0,\min(\gamma_{\mathsf{J1}}^*,\gamma_{\mathsf{Jmax}})\}}\Theta(\gamma_{\mathsf{J}}), \\ \text{if } a>0, b\ge 0, b^2c+a^2e>abd, \\ \min\left[\gamma_{\mathsf{J1}}^*,\gamma_{\mathsf{Jmax}}\right], \text{ if } a>0, b<0, \\ 0, \text{ other cases,} \end{cases} \tag{30}$$

where $\gamma_{\mathsf{J1}}^* = \frac{1}{ac}(bc+\sqrt{b^2c^2+a^2ce-abcd})$.

Proof: The proof is given in Appendix C. ■

From (30), it is observed that Eve operates in the passive mode when (i) the legitimate link has advantages over the eavesdropping link, i.e., $b<0$, and the effect of self-interference is stronger than the jamming link, i.e., $a<0$ and (ii) the eavesdropping link has advantages over the legitimate link, i.e., $b>0$, and the effect of self-interference is stronger than the jamming link, i.e., $a<0$. In the other cases, depending on the situation, Eve chooses her transmit power.

IV. Imperfect Channel Estimation at Eve

In the previous sections, we have investigated the considered system with the assumption of perfect channel estimation at Eve. In this section, the effect of imperfect channel estimation at Eve will be studied.

A. MMSE Channel Estimation for the Jamming Link

In order to perform beamforming from Alice to Bob, both have to exchange their CSI during training sequence. Normally, this information is exchanged via public channel and the framework of training sequence can be known at Eve. Therefore, Eve can perform channel estimation of eavesdropping and jamming links.

Firstly, Bob sends training signals to Alice for enabling Alice creating the pre-code matrix. As a consequence, Eve overhears this information and performs channel estimation for the jamming channel. At Eve, the received signal from Bob is given as

$$\boldsymbol{y}_{\mathsf{J}} = \sqrt{\mathcal{P}_{\mathsf{B}}}\boldsymbol{g}_{\mathsf{J}} x_{sp} + \boldsymbol{w}_{\mathsf{J}}, \tag{31}$$

where x_{sp} is the pilot signal from Bob, $\mathbb{E}\left\{|x_{sp}|^2\right\} = 1$, $\mathcal{P}_{\mathsf{B}}$ is the transmit power of Bob, and $\boldsymbol{w}_{\mathsf{J}} \sim \sigma_0 \mathcal{CN}(0, \boldsymbol{I}_N)$ is the AWGN at Bob. In this work, we assume that the minimal mean square error (MMSE) channel estimation is processed at Eve. The estimated channel from Eve to Bob is given as

$$\hat{\boldsymbol{g}}_{\mathsf{J}} = \mathbb{C}_{\boldsymbol{g}_{\mathsf{J}},\boldsymbol{y}_{\mathsf{J}}} \mathbb{C}^{-1}_{\boldsymbol{y}_{\mathsf{J}},\boldsymbol{y}_{\mathsf{J}}} \boldsymbol{y}_{\mathsf{J}} = \frac{\mathcal{P}_{\mathsf{B}}\beta_{\mathsf{J}}}{\mathcal{P}_{\mathsf{B}}\beta_{\mathsf{J}} + \sigma_0^2}\boldsymbol{g}_{\mathsf{J}} + \frac{\sqrt{\mathcal{P}_{\mathsf{B}}}\beta_{\mathsf{J}}}{\mathcal{P}_{\mathsf{B}}\beta_{\mathsf{J}} + \sigma_0^2}\boldsymbol{w}_{\mathsf{J}} x_{sp}^*, \tag{32}$$

where $\mathbb{C}_{\hat{\boldsymbol{g}}_{\mathsf{J}},\boldsymbol{y}_{\mathsf{J}}} = \sqrt{\mathcal{P}_{\mathsf{B}}}\beta_{\mathsf{J}}\boldsymbol{I}_N x_{sp}^*$, $\mathbb{C}_{\boldsymbol{y}_{\mathsf{J}},\boldsymbol{y}_{\mathsf{J}}} = (\mathcal{P}_{\mathsf{B}}\beta_{\mathsf{J}} + \sigma_0^2)\boldsymbol{I}_N$. From (32), it is observed that $\hat{\boldsymbol{g}}_{\mathsf{J}} \sim \beta_{\mathsf{J}}\sqrt{\frac{\gamma_{\mathsf{B}}}{\gamma_{\mathsf{B}}\beta_{\mathsf{J}}+1}}\mathcal{CN}(0, \boldsymbol{I}_N)$, where $\gamma_{\mathsf{B}} = \frac{\mathcal{P}_{\mathsf{B}}}{\sigma_0^2}$.

We denote the estimation error for the jamming channel as follows:

$$\boldsymbol{\mathcal{E}}_{\mathsf{J}} \triangleq \boldsymbol{g}_{\mathsf{J}} - \hat{\boldsymbol{g}}_{\mathsf{J}} = \frac{\sigma_0^2}{\mathcal{P}_{\mathsf{B}}\beta_{\mathsf{J}} + \sigma_0^2}\boldsymbol{g}_{\mathsf{J}} - \frac{\sqrt{\mathcal{P}_{\mathsf{B}}}\beta_{\mathsf{J}}}{\mathcal{P}_{\mathsf{B}}\beta_{\mathsf{J}} + \sigma_0^2}\boldsymbol{w}_{\mathsf{J}} x_{sp}^*, \tag{33}$$

where $\boldsymbol{\mathcal{E}}_{\mathsf{J}}$ is independent of $\hat{\boldsymbol{g}}_{\mathsf{J}}$ and $\boldsymbol{\mathcal{E}}_{\mathsf{J}} \sim \sqrt{\frac{\beta_{\mathsf{J}}}{\gamma_{\mathsf{B}}\beta_{\mathsf{J}}+1}}\mathcal{CN}(0, \boldsymbol{I}_N)$.

B. MMSE Channel Estimation for the Eavesdropping Link

After receiving the training signals from Bob, Alice sends feedback to Bob to inform the channel state. At the same time, Eve obtains these training signals and performs the channel estimation for the eavesdropping link. The received signal at Eve is formulated as

$$\boldsymbol{y}_{\mathsf{E}} = \sqrt{\mathcal{P}_{\mathsf{A}}}\bar{\boldsymbol{g}}_{\mathsf{E}} x_{sp} + \boldsymbol{w}_{\mathsf{E}}, \tag{34}$$

where $\boldsymbol{w}_{\mathsf{E}} \sim \sigma_0 \mathcal{CN}(0, \boldsymbol{I}_M)$ is the AWGN at Eve. As a consequence, the estimated channel at Eve is

$$\hat{\boldsymbol{g}}_{\mathsf{E}} = \mathbb{C}_{\bar{\boldsymbol{g}}_{\mathsf{E}},\boldsymbol{y}_{\mathsf{E}}} \mathbb{C}^{-1}_{\boldsymbol{y}_{\mathsf{E}},\boldsymbol{y}_{\mathsf{E}}} \boldsymbol{y}_{\mathsf{E}} = \frac{\mathcal{P}_{\mathsf{A}}\beta_{\mathsf{E}}}{\mathcal{P}_{\mathsf{A}}\beta_{\mathsf{E}} + \sigma_0^2}\bar{\boldsymbol{g}}_{\mathsf{E}} + \frac{\sqrt{\mathcal{P}_{\mathsf{A}}}\beta_{\mathsf{E}}}{\mathcal{P}_{\mathsf{A}}\beta_{\mathsf{E}} + \sigma_0^2}\boldsymbol{w}_{\mathsf{E}} x_{sp}^*, \tag{35}$$

where $\mathbb{C}$ is the covariance matrix, $\mathbb{C}_{\bar{\boldsymbol{g}}_{\mathsf{E}},\boldsymbol{y}_{\mathsf{E}}} = \sqrt{\mathcal{P}_{\mathsf{A}}}\beta_{\mathsf{E}}\boldsymbol{I}_M x_{sp}^*$, $\mathbb{C}_{\boldsymbol{y}_{\mathsf{E}},\boldsymbol{y}_{\mathsf{E}}} = (\mathcal{P}_{\mathsf{A}}\beta_{\mathsf{E}} + \sigma_0^2)\boldsymbol{I}_M$. As observing (35), $\hat{\boldsymbol{g}}_{\mathsf{E}} \sim \beta_{\mathsf{E}}\sqrt{\frac{\gamma_{\mathsf{A}}}{\gamma_{\mathsf{A}}\beta_{\mathsf{E}}+1}}\mathcal{CN}(0, \boldsymbol{I}_M)$.

We denote the estimation error for the eavesdropping channel as

$$\boldsymbol{\mathcal{E}}_{\mathsf{E}} \triangleq \bar{\boldsymbol{g}}_{\mathsf{E}} - \hat{\boldsymbol{g}}_{\mathsf{E}} = \frac{\sigma_0^2}{\mathcal{P}_{\mathsf{A}}\beta_{\mathsf{E}} + \sigma_0^2}\bar{\boldsymbol{g}}_{\mathsf{E}} - \frac{\sqrt{\mathcal{P}_{\mathsf{A}}}\beta_{\mathsf{E}}}{\mathcal{P}_{\mathsf{A}}\beta_{\mathsf{E}} + \sigma_0^2}\boldsymbol{w}_{\mathsf{E}} x_{sp}^*. \tag{36}$$

It is worth noting that because of the property of MMSE estimation, $\boldsymbol{\mathcal{E}}_{\mathsf{E}}$ is independent of $\hat{\boldsymbol{g}}_{\mathsf{E}}$ and $\boldsymbol{\mathcal{E}}_{\mathsf{E}} \sim \sqrt{\frac{\beta_{\mathsf{E}}}{\gamma_{\mathsf{A}}\beta_{\mathsf{E}}+1}}\mathcal{CN}(0, \boldsymbol{I}_N)$.

C. Closed-form Expression for Finite K, M, N

1) Ergodic Legitimate Rate: After having the estimated channel of the jamming channel, Eve creates beamforming to Bob. The jamming signal from Eve is designed as

$$s_{\mathsf{J}} = \sqrt{\mathcal{P}_{\mathsf{J}}}\frac{\hat{\boldsymbol{g}}_{\mathsf{J}}}{\|\hat{\boldsymbol{g}}_{\mathsf{J}}\|} x_{\mathsf{J}}, \tag{37}$$

Therefore, the received signal at Bob can be formulated as

$$y_{\mathsf{L}} = \sqrt{\mathcal{P}_{\mathsf{A}}}\,\|\boldsymbol{g}_{\mathsf{L}}\|\,x + \sqrt{\mathcal{P}_{\mathsf{J}}}\,\|\hat{\boldsymbol{g}}_{\mathsf{J}}\|\,x_{\mathsf{J}} + \sqrt{\mathcal{P}_{\mathsf{J}}}\boldsymbol{\mathcal{E}}_{\mathsf{J}}^H \frac{\hat{\boldsymbol{g}}_{\mathsf{J}}}{\|\hat{\boldsymbol{g}}_{\mathsf{J}}\|} x_{\mathsf{J}} + w_{\mathsf{L}}. \tag{38}$$

From (38), when imperfect channel estimation is considered at Eve, the ergodic rate of the legitimate channel can be formulated as

$$\begin{aligned}\hat{R}_{\mathsf{L}} &= \mathbb{E}\left\{\log_2\left(1 + \frac{\mathcal{P}_{\mathsf{A}}\|\boldsymbol{g}_{\mathsf{L}}\|^2}{\mathcal{P}_{\mathsf{J}}\left(\mathbb{E}\left\{\|\hat{\boldsymbol{g}}_{\mathsf{J}}\|^2\right\} + \mathbb{E}\left\{\left|\boldsymbol{\mathcal{E}}_{\mathsf{J}}^H \frac{\hat{\boldsymbol{g}}_{\mathsf{J}}}{\|\hat{\boldsymbol{g}}_{\mathsf{J}}\|}\right|^2\right\}\right) + \sigma_0^2}\right)\right\} \\ &= \mathbb{E}\left\{\log_2\left(1 + \frac{\gamma_{\mathsf{A}}\|\boldsymbol{g}_{\mathsf{L}}\|^2}{\frac{\gamma_{\mathsf{J}}\gamma_{\mathsf{B}}\beta_{\mathsf{J}}^2 N}{\gamma_{\mathsf{B}}\beta_{\mathsf{J}}+1} + \frac{\gamma_{\mathsf{J}}\beta_{\mathsf{J}}}{\gamma_{\mathsf{B}}\beta_{\mathsf{J}}+1} + 1}\right)\right\}\end{aligned} \tag{39}$$

From (39), the following lemmas are given.

Lemma 6: When imperfect channel estimation is considered at Eve, the exact closed-form for ergodic rate of the legitimate channel is given as

$$\begin{aligned}\hat{R}_{\mathsf{L}} = &\frac{1}{\ln 2}\sum_{k=0}^{K-1}\frac{1}{(K-1-k)!} \\ &\times \left(-\frac{\gamma_{\mathsf{J}}\gamma_{\mathsf{B}}\beta_{\mathsf{J}}^2 N + \gamma_{\mathsf{J}}\beta_{\mathsf{J}} + \gamma_{\mathsf{B}}\beta_{\mathsf{J}} + 1}{\gamma_{\mathsf{A}}\beta_{\mathsf{L}}(\gamma_{\mathsf{B}}\beta_{\mathsf{J}} + 1)}\right)^{K-k-1} \\ &\times \left[-\exp\left(\frac{\gamma_{\mathsf{J}}\gamma_{\mathsf{B}}\beta_{\mathsf{J}}^2 N + \gamma_{\mathsf{J}}\beta_{\mathsf{J}} + \gamma_{\mathsf{B}}\beta_{\mathsf{J}} + 1}{\gamma_{\mathsf{A}}\beta_{\mathsf{L}}(\gamma_{\mathsf{B}}\beta_{\mathsf{J}} + 1)}\right)\right. \\ &\times \mathrm{Ei}\left(-\frac{\gamma_{\mathsf{J}}\gamma_{\mathsf{B}}\beta_{\mathsf{J}}^2 N + \gamma_{\mathsf{J}}\beta_{\mathsf{J}} + \gamma_{\mathsf{B}}\beta_{\mathsf{J}} + 1}{\gamma_{\mathsf{A}}\beta_{\mathsf{L}}(\gamma_{\mathsf{B}}\beta_{\mathsf{J}} + 1)}\right) \\ &\left. + \sum_{l=1}^{K-k-1}(l-1)!\left(-\frac{\gamma_{\mathsf{J}}\gamma_{\mathsf{B}}\beta_{\mathsf{J}}^2 N + \gamma_{\mathsf{J}}\beta_{\mathsf{J}} + \gamma_{\mathsf{B}}\beta_{\mathsf{J}} + 1}{\gamma_{\mathsf{A}}\beta_{\mathsf{L}}(\gamma_{\mathsf{B}}\beta_{\mathsf{J}} + 1)}\right)^{-l}\right].\end{aligned} \tag{40}$$

Lemma 7: When imperfect channel estimation is considered at Eve, the approximation for the ergodic rate of the legitimate channel is formulated as follows:

$$\hat{R}_{\mathsf{L}} \approx \hat{R}_{\mathsf{L}}^a \triangleq \log_2\left(1 + \frac{\gamma_{\mathsf{A}} K \beta_{\mathsf{L}}}{\gamma_{\mathsf{J}}\beta_{\mathsf{J}} N\frac{\gamma_{\mathsf{B}}\beta_{\mathsf{J}}}{(\gamma_{\mathsf{B}}\beta_{\mathsf{J}}+1)} + \frac{\gamma_{\mathsf{J}}\beta_{\mathsf{J}}}{(\gamma_{\mathsf{B}}\beta_{\mathsf{J}}+1)} + 1}\right). \tag{41}$$

Eq. (41) is obtained by using the identity (13).

Remark 4: From (41), we can observe that

$$\hat{R}_{\mathsf{L}}^{a} \overset{\gamma_{\mathsf{B}}\to\infty}{\to} \log_2\left(1+\frac{\gamma_{\mathsf{A}}\beta_{\mathsf{L}}K}{\gamma_{\mathsf{J}}\beta_{\mathsf{J}}N+1}\right), \tag{42}$$

which is similar to (12). In other words, Eve can benefit from the high transmit power at Bob. Besides, another observation is as follows:

$$\hat{R}_{\mathsf{L}}^{a} \overset{\gamma_{\mathsf{B}}\to 0}{\to} \log_2\left(1+\frac{\gamma_{\mathsf{A}}\beta_{\mathsf{L}}K}{\gamma_{\mathsf{J}}\beta_{\mathsf{J}}+1}\right), \tag{43}$$

which means that when Bob uses a very small transmit power to make the channel estimation process at Eve difficult, malicious attack benefits from increasing the transmit power but loses the advantage of the number of transmit antennas at Eve.

2) Ergodic Eavesdropping Rate: Within the full-duplex mode, at the receive antennas, Eve receives her jamming signal. Therefore, the received signals at Eve is formulated as

$$\boldsymbol{y}_{\mathsf{E}} = \sqrt{\mathcal{P}_{\mathsf{A}}}\bar{\boldsymbol{g}}_{\mathsf{E}}x + \sqrt{\mathcal{P}_{\mathsf{J}}}\boldsymbol{G}_{\mathsf{I}}\frac{\hat{\boldsymbol{g}}_{\mathsf{J}}}{\|\hat{\boldsymbol{g}}_{\mathsf{J}}\|}x_{\mathsf{J}} + \boldsymbol{w}_{\mathsf{E}}, \tag{44}$$

After performing channel estimation, Eve deploys MRC technique to process the received signals. Consequently, the received signal at Eve after MRC process is given as

$$\begin{aligned} y_{\mathsf{E}}^{\mathsf{MRC}} = \sqrt{\mathcal{P}_{\mathsf{A}}}\,\|\hat{\boldsymbol{g}}_{\mathsf{E}}\|\,x + \sqrt{\mathcal{P}_{\mathsf{A}}}\frac{\hat{\boldsymbol{g}}_{\mathsf{E}}^{H}}{\|\hat{\boldsymbol{g}}_{\mathsf{E}}\|}\boldsymbol{\mathcal{E}}_{\mathsf{E}}x + \sqrt{\mathcal{P}_{\mathsf{J}}}\frac{\hat{\boldsymbol{g}}_{\mathsf{E}}^{H}}{\|\hat{\boldsymbol{g}}_{\mathsf{E}}\|}\hat{\boldsymbol{g}}_{\mathsf{I}}x_{\mathsf{J}} \\ + \frac{\hat{\boldsymbol{g}}_{\mathsf{E}}^{H}}{\|\hat{\boldsymbol{g}}_{\mathsf{E}}\|}\boldsymbol{w}_{\mathsf{E}}, \end{aligned} \tag{45}$$

where $\hat{\boldsymbol{g}}_{\mathsf{I}} = \boldsymbol{G}_{\mathsf{I}}\frac{\hat{\boldsymbol{g}}_{\mathsf{J}}}{\|\hat{\boldsymbol{g}}_{\mathsf{J}}\|}$ and $\hat{\boldsymbol{g}}_{\mathsf{I}} \sim \sigma_{\mathsf{I}}\,\mathcal{CN}(0,\boldsymbol{I}_M)$.

Alice considers the estimated channel as the true channel and the last three terms in (45) as the interference and noise. Therefore, the ergodic eavesdropping rate is given in (46) on the top of the next page. Step (a) in (46) is obtained by using the properties of circularly symmetric normal vectors $\frac{\hat{\boldsymbol{g}}_{\mathsf{E}}^{H}}{\|\hat{\boldsymbol{g}}_{\mathsf{E}}\|}\boldsymbol{\mathcal{E}}_{\mathsf{E}} \sim \mathcal{CN}\left(0,\frac{\beta_{\mathsf{E}}}{\gamma_{\mathsf{A}}\beta_{\mathsf{E}}+1}\right)$, $\frac{\hat{\boldsymbol{g}}_{\mathsf{E}}^{H}}{\|\hat{\boldsymbol{g}}_{\mathsf{E}}\|}\hat{\boldsymbol{g}}_{\mathsf{I}} \sim \mathcal{CN}(0,\sigma_{\mathsf{I}}^2)$, $\frac{\hat{\boldsymbol{g}}_{\mathsf{E}}^{H}}{\|\hat{\boldsymbol{g}}_{\mathsf{E}}\|}\boldsymbol{w}_{\mathsf{E}} \sim \mathcal{CN}(0,\sigma_0^2)$, and the identity (13).

From (46), the following lemmas are given.

Lemma 8: When imperfect channel estimation is considered at Eve, the exact closed-form expression for the ergodic eavesdropping rate is formulated as follows:

$$\begin{aligned} \hat{R}_{\mathsf{E}} = \frac{1}{\ln 2}\sum_{m=0}^{M-1}\frac{1}{(M-m-1)!} \\ \times\left(-\frac{(\gamma_{\mathsf{A}}\beta_{\mathsf{E}}+1)(\gamma_{\mathsf{J}}\sigma_{\mathsf{I}}^2+1)+\gamma_{\mathsf{A}}\beta_{\mathsf{E}}}{\gamma_{\mathsf{A}}^2\beta_{\mathsf{E}}^2}\right)^{M-m-1} \\ \times\left[-\exp\left(\frac{(\gamma_{\mathsf{A}}\beta_{\mathsf{E}}+1)(\gamma_{\mathsf{J}}\sigma_{\mathsf{I}}^2+1)+\gamma_{\mathsf{A}}\beta_{\mathsf{E}}}{\gamma_{\mathsf{A}}^2\beta_{\mathsf{E}}^2}\right)\right. \\ \times\mathrm{Ei}\left(-\frac{(\gamma_{\mathsf{A}}\beta_{\mathsf{E}}+1)(\gamma_{\mathsf{J}}\sigma_{\mathsf{I}}^2+1)+\gamma_{\mathsf{A}}\beta_{\mathsf{E}}}{\gamma_{\mathsf{A}}^2\beta_{\mathsf{E}}^2}\right) \\ \left.+\sum_{p=1}^{M-m-1}(p-1)!\left(-\frac{(\gamma_{\mathsf{A}}\beta_{\mathsf{E}}+1)(\gamma_{\mathsf{J}}\sigma_{\mathsf{I}}^2+1)+\gamma_{\mathsf{A}}\beta_{\mathsf{E}}}{\gamma_{\mathsf{A}}^2\beta_{\mathsf{E}}^2}\right)^{-p}\right]. \end{aligned} \tag{47}$$

Proof: The proof is given in Appendix D. ∎

Lemma 9: When imperfect channel estimation is considered at Eve, the approximation of the ergodic eavesdropping rate is given as

$$\hat{R}_{\mathsf{E}} \approx \hat{R}_{\mathsf{E}}^{\mathsf{a}} \triangleq \log_2\left(1+\frac{\gamma_{\mathsf{A}}\beta_{\mathsf{E}}M}{\frac{\gamma_{\mathsf{A}}\beta_{\mathsf{E}}}{\gamma_{\mathsf{A}}\beta_{\mathsf{E}}+1}+\gamma_{\mathsf{J}}\sigma_{\mathsf{I}}^2+1}\right). \tag{48}$$

Proof: Eq. (48) is obtained by using identity (13). ∎

Similar to the perfect channel estimation scheme, the ergodic eavesdropping rate in the imperfect channel estimation scheme depends on the transmit power but does not depend on the number of transmit antennas at Eve. In addition, as the transmit power at Alice is high, (48) approximates (17). Therefore, the channel estimation process at Eve benefits from increasing the transmit power at Alice.

3) Achievable Ergodic Secrecy Rate: The exact-closed form expression of the achivable ergodic secrecy rate can be calculated directly from (40) and (47) as follows:

$$\hat{R}_{\mathsf{S}} = [\hat{R}_{\mathsf{L}} - \hat{R}_{\mathsf{E}}]^{+}. \tag{49}$$

From (41) and (48), the approximation for the achievable ergodic secrecy rate of the considered system is expressed as

$$\hat{R}_{\mathsf{S}}^{\mathsf{a}} \triangleq [\hat{R}_{\mathsf{L}}^{\mathsf{a}} - \hat{R}_{\mathsf{E}}^{\mathsf{a}}]^{+} = \left[\log_2(\hat{\Psi})\right]^{+}, \tag{50}$$

where

$$\begin{aligned} \hat{\Psi} = \frac{\left[\gamma_{\mathsf{J}}\gamma_{\mathsf{B}}\beta_{\mathsf{J}}^2N+\gamma_{\mathsf{J}}\beta_{\mathsf{J}}+\gamma_{\mathsf{B}}\beta_{\mathsf{J}}+1+\gamma_{\mathsf{A}}\beta_{\mathsf{L}}K(\gamma_{\mathsf{B}}\beta_{\mathsf{J}}+1)\right]}{\left[\gamma_{\mathsf{J}}\gamma_{\mathsf{B}}\beta_{\mathsf{J}}^2N+\gamma_{\mathsf{J}}\beta_{\mathsf{J}}+\gamma_{\mathsf{B}}\beta_{\mathsf{J}}+1\right]} \\ \times\frac{\left[\gamma_{\mathsf{A}}\beta_{\mathsf{E}}+(1+\gamma_{\mathsf{J}}\sigma_{\mathsf{I}}^2)(\gamma_{\mathsf{A}}\beta_{\mathsf{E}}+1)\right]}{\left[\gamma_{\mathsf{A}}\beta_{\mathsf{E}}(M+1)+(1+\gamma_{\mathsf{J}}\sigma_{\mathsf{I}}^2)(\gamma_{\mathsf{A}}\beta_{\mathsf{E}}+1)+\gamma_{\mathsf{A}}^2\beta_{\mathsf{E}}^2M\right]}. \end{aligned} \tag{51}$$

Lemma 10: The asymptotic expression of the achievable ergodic secrecy rate when transmit power at Alice is high with imperfect channel estimation at Eve is given as follows:

$$\hat{R}_{\mathsf{s}}^{\mathsf{u,asym}} \overset{\gamma_{\mathsf{A}}\to\infty}{\to} \left[\log_2\left(\frac{K\beta_{\mathsf{L}}(\gamma_{\mathsf{B}}\beta_{\mathsf{J}}+1)(\gamma_{\mathsf{J}}\sigma_{\mathsf{I}}^2+2)}{[\gamma_{\mathsf{J}}\beta_{\mathsf{J}}(\gamma_{\mathsf{B}}\beta_{\mathsf{J}}N+1)+\gamma_{\mathsf{B}}\beta_{\mathsf{J}}+1]\beta_{\mathsf{E}}M}\right)\right]^{+}. \tag{52}$$

Remark 5: When imperfect channel estimation is considered at Eve, increasing transmit power at Alice still cannot guarantee an improvement in secrecy performance for the legitimate side. Besides, increasing the numbers of transmit and receive antennas at Eve can reduce the effect of the self-interference and imperfect channel estimation on the malicious attack.

D. Asymptotic Analysis

1) Power Scale Law at Eve: When imperfect channel estimation is considered at Eve, the power scale law still holds true at Eve, i.e., the transmit power at Eve can be reduced proportionally to $\left(\frac{1}{N}\right)^{\mu}$, where $0<\mu<1$.

Proof: Plugging $\gamma_{\mathsf{J}} = \frac{\bar{\gamma}_{\mathsf{J}}}{N^{\mu}}$ into (50), where $\bar{\gamma}_{\mathsf{J}}$ is the maximal transmit power of Eve. When the number of transmit antennas at Eve, i.e, N is large, $\hat{\Psi}$ can be rewritten as

$$\hat{\Psi} \overset{N\to\infty}{\to} \frac{2\gamma_{\mathsf{A}}\beta_{\mathsf{E}}+1}{\gamma_{\mathsf{A}}\beta_{\mathsf{E}}(M+2)+1+\gamma_{\mathsf{A}}^2\beta_{\mathsf{E}}^2M} < 1, \tag{53}$$

$$\hat{R}_{\mathsf{E}} = \mathbb{E}\left\{\log_2\left(1+\frac{\mathcal{P}_{\mathsf{A}}\left\|\hat{\boldsymbol{g}}_{\mathsf{E}}\right\|^2}{\mathcal{P}_{\mathsf{A}}\mathbb{E}\left\{\left|\frac{\hat{\boldsymbol{g}}_{\mathsf{E}}^H}{\|\hat{\boldsymbol{g}}_{\mathsf{E}}\|}\boldsymbol{\mathcal{E}}_{\mathsf{E}}\right|^2\right\}+\mathcal{P}_{\mathsf{J}}\mathbb{E}\left\{\left|\frac{\hat{\boldsymbol{g}}_{\mathsf{E}}^H}{\|\hat{\boldsymbol{g}}_{\mathsf{E}}\|}\hat{\boldsymbol{g}}_{\mathsf{I}}\right|^2\right\}+\mathbb{E}\left\{\left|\frac{\hat{\boldsymbol{g}}_{\mathsf{E}}^H}{\|\hat{\boldsymbol{g}}_{\mathsf{E}}\|}\boldsymbol{w}_{\mathsf{E}}\right|^2\right\}}\right)\right\} \overset{(a)}{=} \mathbb{E}\left\{\log_2\left(1+\frac{\gamma_{\mathsf{A}}\left\|\hat{\boldsymbol{g}}_{\mathsf{E}}\right\|^2}{\frac{\gamma_{\mathsf{A}}\beta_{\mathsf{E}}}{\gamma_{\mathsf{A}}\beta_{\mathsf{E}}+1}+\gamma_{\mathsf{J}}\sigma_{\mathsf{I}}^2+1}\right)\right\}. \tag{46}$$

which guarantees that $\hat{R}_{\mathsf{S}} = 0$. ■

Although suffering from imperfect channel estimation, Eve can reduce her transmit power by increasing her number of transmit antennas, followed by a reduction in the effect of self-interference.

2) Rule for the Number of Antennas at Eve: When imperfect channel estimation is taken into account at Eve and the transmit power at Alice and Eve is high, the number of antennas at Eve for guaranteeing $\hat{R}_{\mathsf{s}} = 0$ is constrained as

$$\nu > 1 + \log\left(\frac{\beta_{\mathsf{L}}\sigma_{\mathsf{I}}^2(\gamma_{\mathsf{B}}\beta_{\mathsf{J}}+1)}{\beta_{\mathsf{J}}\beta_{\mathsf{E}}\epsilon_m(\gamma_{\mathsf{B}}\beta_{\mathsf{J}}\epsilon_n K^{\alpha}+1)}\right)\frac{1}{\log(K)}, \tag{54}$$

where $N = \epsilon_n K^{\alpha}$, $M = \epsilon_m K^{\nu}$, $\gamma_{\mathsf{J}} = \varrho\gamma_{\mathsf{A}}$, $\epsilon_m > 0$, $\epsilon_n > 0$, $\alpha > 0$, $\nu > 0$, and $\varrho > 0$.

As been observed from (54), when Bob uses small transmit power, (54) becomes the condition for the number of receive antennas at Eve as follows:

$$\nu > 1 + \log\left(\frac{\beta_{\mathsf{L}}\sigma_{\mathsf{I}}^2}{\beta_{\mathsf{J}}\beta_{\mathsf{E}}\epsilon_m}\right)\frac{1}{\log(K)}. \tag{55}$$

We also observe that when Bob uses high transmit power, (54) becomes (25).

E. Transmit Power Optimization Scheme for Cyber-weapon

Similar to the perfect channel estimation scheme, the optimization problem can be formulated as

$$\begin{aligned} \min_{\gamma_{\mathsf{J}}} \quad & \hat{R}_{\mathsf{E}}^{\mathsf{a}} - \hat{R}_{\mathsf{L}}^{\mathsf{a}} \\ \text{s. t.} \quad & \hat{R}_{\mathsf{E}}^{\mathsf{a}} > \hat{R}_{\mathsf{L}}^{\mathsf{a}}, \qquad (56) \\ & 0 \le \gamma_{\mathsf{J}} \le \gamma_{\mathsf{Jmax}}, \qquad (57) \end{aligned}$$

where R_{th} is the pre-defined target rate of the eavesdropping channel and γ_{Jmax} is the maximal transmit power of Eve. From (56), an equivalent optimization problem can be expressed as

$$\begin{aligned} \min_{\gamma_{\mathsf{J}}} \quad & \hat{\Theta}(\gamma_{\mathsf{J}}) \\ \text{s. t.} \quad & \hat{a}\gamma_{\mathsf{J}} + \hat{\gamma}_{\mathsf{B}} > 0, \qquad (58) \\ & 0 \le \gamma_{\mathsf{J}} \le \gamma_{\mathsf{Jmax}}, \qquad (59) \end{aligned}$$

where $\hat{\Theta}(\gamma_{\mathsf{J}}) = 1 + \frac{\hat{a}\gamma_{\mathsf{J}}+\hat{b}}{\hat{c}\gamma_{\mathsf{J}}^2+\hat{d}\gamma_{\mathsf{J}}+\hat{e}}$, $\hat{a} = \gamma_{\mathsf{A}}\beta_{\mathsf{E}}M\beta_{\mathsf{J}}(\gamma_{\mathsf{A}}\beta_{\mathsf{E}}+1)(\gamma_{\mathsf{B}}\beta_{\mathsf{J}}N+1) - \gamma_{\mathsf{A}}K\beta_{\mathsf{L}}\sigma_{\mathsf{I}}^2(\gamma_{\mathsf{A}}\beta_{\mathsf{E}}+1)(\gamma_{\mathsf{B}}\beta_{\mathsf{J}}+1)$, $\hat{b} = \gamma_{\mathsf{A}}(\gamma_{\mathsf{B}}\beta_{\mathsf{J}}+1)[(\gamma_{\mathsf{A}}\beta_{\mathsf{E}}+1)\beta_{\mathsf{E}}M - (2\gamma_{\mathsf{A}}\beta_{\mathsf{E}}+1)K\beta_{\mathsf{L}}]$, $\hat{c} = \beta_{\mathsf{J}}\sigma_{\mathsf{I}}^2(\gamma_{\mathsf{A}}\beta_{\mathsf{E}}+1)(\gamma_{\mathsf{B}}\beta_{\mathsf{J}}N+1)$, $\hat{d} = (2\gamma_{\mathsf{A}}\beta_{\mathsf{E}}+1)(\gamma_{\mathsf{B}}\beta_{\mathsf{J}}N+1)\beta_{\mathsf{J}} + \sigma_{\mathsf{I}}^2(\gamma_{\mathsf{A}}\beta_{\mathsf{E}}+1)(\gamma_{\mathsf{B}}\beta_{\mathsf{J}}+1)(\gamma_{\mathsf{A}}K\beta_{\mathsf{L}}+1)$, and $\hat{e} = (\gamma_{\mathsf{B}}\beta_{\mathsf{J}}+1)(\gamma_{\mathsf{A}}K\beta_{\mathsf{L}}+1)(2\gamma_{\mathsf{A}}\beta_{\mathsf{E}}+1)$.

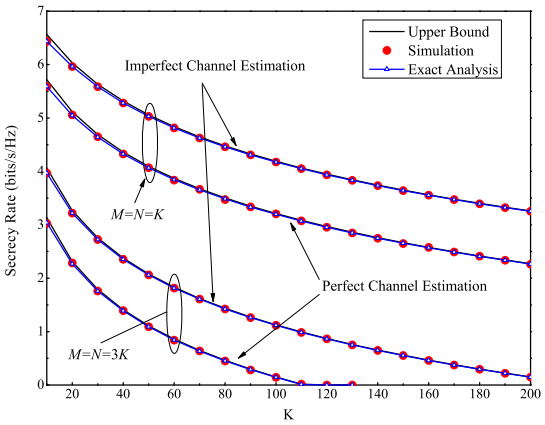

Fig. 2: Secrecy rate versus the number of antennas at Alice.

The optimal solution for transmit power γ_{J}^* is as follows:

$$\gamma_{\mathsf{J}}^* = \begin{cases} \arg \max\limits_{\gamma_{\mathsf{J}}\in\{0,\min(\gamma_{\mathsf{J1}}^*,\gamma_{\mathsf{Jmax}})\}} \hat{\Theta}(\gamma_{\mathsf{J}}), \\ \text{if } \hat{a}>0, \hat{b}\ge 0, \hat{b}^2\hat{c}+\hat{a}^2\hat{e} > \hat{a}\hat{b}\hat{d}, \\ \min\left[\gamma_{\mathsf{J1}}^*, \gamma_{\mathsf{Jmax}}\right], \text{ if } \hat{a}>0, \hat{b}<0, \\ 0, \text{ other cases}, \end{cases} \tag{60}$$

where $\gamma_{\mathsf{J1}}^* = \frac{1}{\hat{a}\hat{c}}(\hat{b}\hat{c} + \sqrt{\hat{b}^2\hat{c}^2+\hat{a}^2\hat{c}\hat{e}-\hat{a}\hat{b}\hat{c}\hat{d}})$.

Proof: The proof follows a similar method as given in Appendix C. ■

V. Numerical Results

In this section, we first provide numerical results based on Monte-Carlo simulation to evaluate the tightness of our approximation for the ergodic secrecy rate.

In Fig. 2, comparisons among simulation, closed-form, and the approximation of the achievable ergodic secrecy rate in the perfect and imperfect channel estimation schemes are demonstrated respectively. In this setup, the number of transmit antennas at Alice, the number of receive antennas and the number of transmit antennas at Eve are set at $M = N = K$ and $M = N = 3K$, the transmit power of Alice is set at $\gamma_{\mathsf{A}} = 30$ dB, the transmit power of Eve is set at $\gamma_{\mathsf{J}} = 20$ dB, the transmit power of Bob is set at $\gamma_{\mathsf{B}} = 10$ dB, $\beta_{\mathsf{E}} = 1$, $\beta_{\mathsf{L}} = 1$, $\beta_{\mathsf{J}} = 10^{-1}$, and $\sigma_{\mathsf{I}} = 10$. We can observe that the approximation are tight, especially at large numbers of antennas. Therefore, we use these approximations for the following numerical work. In addition, from the figure, as the number of antennas at Eve is large, the achievable ergodic secrecy rate decreases. The phenomenon can be explained from (12)(for the case of perfect channel estimation at Eve) and (41)(for the case of imperfect channel estimation at Eve). As setting the number of transmit antennas at Eve, i.e., N,

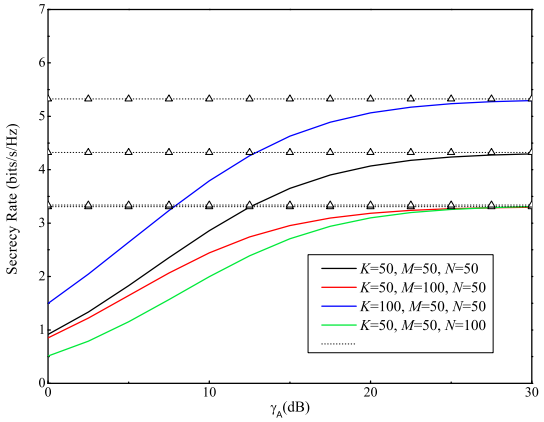

Fig. 3: Secrecy rate with different numbers of antennas and perfect CSI

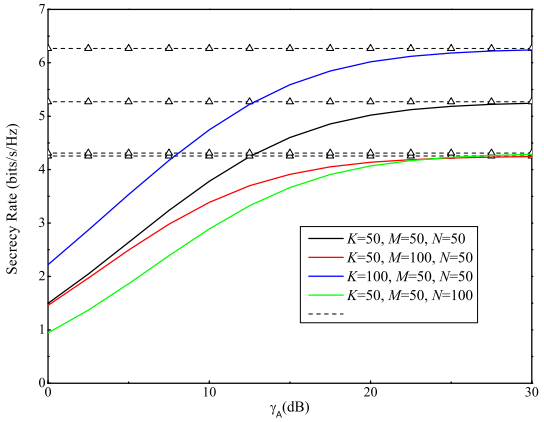

Fig. 4: Secrecy rate with different numbers of antennas and imperfect CSI

proportional to the number of transmit antennas at Alice, i.e., K, the legitimate rate will reduce if the proportion increases. Besides, from (17) and (48), as the number of receive antennas at Eve, i.e., M, increases, the eavesdropping rate increases. As a consequence, the secrecy rate of the considered system reduces when M and N are set proportional to K and K increases. Besides, under the effect of imperfect channel estimation at Eve, the malicious attack is less effective.

Fig. 3 and Fig. 4 show the effect of the numbers of antennas at Alice and Eve on the achievable ergodic secrecy rate of the considered system in the perfect and imperfect channel estimation schemes, respectively. In this setup, $K = \{50, 100\}$, $M = \{50, 100\}$, $N = \{50, 100\}$, $\beta_{\mathsf{L}} = \beta_{\mathsf{E}} = 1$, $\beta_{\mathsf{J}} = 0.1$, $\sigma_{\mathsf{I}} = 10$, $\gamma_{\mathsf{J}} = 10$ dB, $\gamma_{\mathsf{B}} = 10$ dB. As increasing the transmit power at Alice, the achievable ergodic secrecy rate increases and then saturates. The reason is that although increasing transmit power can help legitimate link to decrease the effect of jamming signal from Eve, it also enables Eve to eavesdrop more information. In addition, in the imperfect channel estimation scheme, a greater transmit power at Alice also enhances the channel estimation process at Eve. Therefore, in the legitimate side's point of view, raising the transmit power does not guarantee an improvement in secrecy performance. However, increasing the number of antennas at Alice can enhance the ergodic secrecy rate. At the illegitimate side,

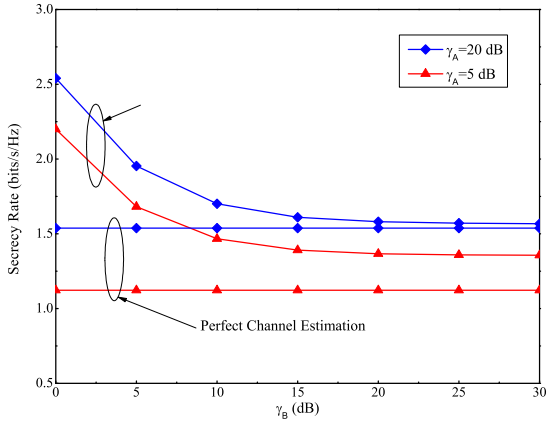

Fig. 5: Effect of transmit power at Bob on the secrecy rate.

raising the number of either transmit or receive antennas can decrease the secrecy performance of legitimate side. Besides, the results have shown that the higher the transmit power at Alice is, the better the effect of increasing the number of receive antennas at Eve is. Meanwhile, deploying a higher number of transmit antennas at Eve significantly decreases the ergodic secrecy rate of the considered system.

Fig. 5 demonstrates the effect of the transmit power at Bob on the ergodic secrecy rate of the considered system. System parameters are set as $K = 100$, $M = 50$, $N = 70$, $\beta_{\mathsf{L}} = 5$, $\beta_{\mathsf{J}} = 0.5$, $\beta_{\mathsf{E}} = 1$, $\sigma_{\mathsf{I}} = 2$, $\gamma_{\mathsf{J}} = 5$ dB and $\gamma_{\mathsf{A}} = \{0, 10, 20\}$ dB. As increasing the transmit power at Bob, the ergodic secrecy rate decreases. The explanation is that when the transmit power at Bob increases, the error of the channel estimation process at Eve for the jamming channel decreases. Therefore, the jamming process at Eve is more effective followed by a reduction in the ergodic secrecy rate.

In Fig. 6, the power scale law of the number of transmit antennas at Eve in the perfect and imperfect channel estimation schemes is presented. In this figure, the transmit power at Eve that satisfies $R_{\mathsf{E}} = R_{\mathsf{M}}$ versus the number of transmit antennas at Eve is plotted. The system parameters are set $\gamma_{\mathsf{A}} = \gamma_{\mathsf{B}} = 1$ dB, $M = 30$, $K = 50, 60, 70$, $\beta_{\mathsf{L}} = \beta_{\mathsf{E}} = \beta_{\mathsf{J}} = 1$, and $\sigma_{\mathsf{I}} = 1$. It is observed that when the number of transmit antennas at Eve is double, the required transmit power at Eve is reduced approximately by 3 dB.

Fig. 7 and Fig. 8 plot the difference between R_{E} and R_{L} versus γ_{A} in the perfect and imperfect channel estimation schemes. The system is configured as $M = 50$, $N = 50$, $\beta_{\mathsf{L}} = \beta_{\mathsf{E}} = \beta_{\mathsf{J}} = 1$, $\sigma_{\mathsf{I}} = 1$, $\gamma_{\mathsf{Jmax}} = 15$ dB, and $\gamma_{\mathsf{B}} = 30$ dB. We consider three cases (i) the cyber-weapon uses the fixed transmit power for jamming, (ii) the cyber-weapon deploys transmit power optimization scheme for jamming based on the statistical CSI, and (iii) the simulation of the case when the cyber-weapon implements transmit power optimization scheme based on the instantaneous CSI [6]. The power optimization scheme based on the instantaneous CSI is performed

[6]From Eve's point of view, it is very hard or almost impossible to obtain the instantaneous CSI of the channel from Alice to Bob for optimizing its transmit power.

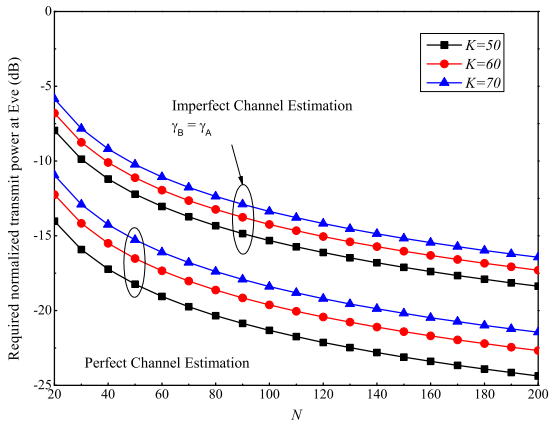

Fig. 6: Power scale law at Eve.

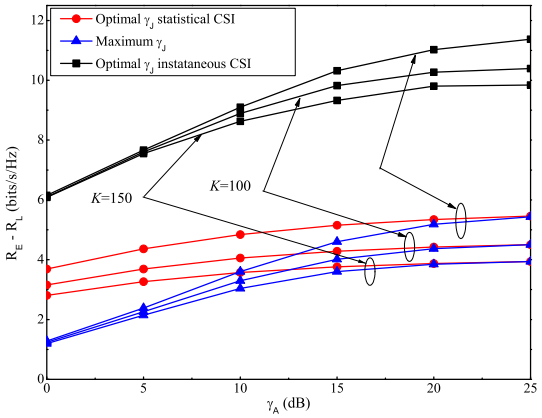

Fig. 7: Power optimization at Eve with perfect CSI

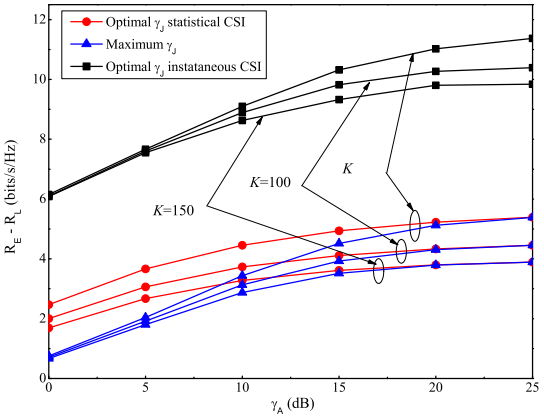

Fig. 8: Power optimization at Eve wiht imperfect CSI

as follows:

$$\max_{\gamma_J} \quad R_E^{inst} - R_L^{inst}$$
$$\text{s. t.} \quad R_E^{inst} > R_L^{inst}, \tag{61}$$
$$0 \le \gamma_J \le \gamma_{Jmax}. \tag{62}$$

From the figures, the case of optimal transmit power with the instantaneous CSI outperforms the other cases at the expense of the full system's CSI knowledge. It is obviously that by using the instantaneous CSI, Eve can adjust her transmit power more quickly followed by a better performance [7]. The case of optimal transmit power with the statistical CSI shows higher $R_E - R_L$ than that in the maximum transmit power case as the transmit power at Alice decreases. The reason is that when the transmit power at Alice is small, the transmit power of Eve in the optimal transmit power case can be decreased to reduce the effect of the self-interference, followed by an enhancement in the eavesdropping rate. Meanwhile, when the transmit power at Alice is high, both Alice and Eve receive more information. In this situation, Eve increases her transmit power to degrade the legitimate channel. Besides, increasing the number of antennas at Alice can restrain the effectiveness of the power optimization scheme at Eve.

In Fig. 9, the performance comparison of the proposed cyber-weapon, a massive array eavesdropper, and a massive array jammer is shown. In this setup, three adversaries have the same number of antennas, i.e., the massive array eavesdropper and jammer are equipped with 100 antennas, the cyber-weapon is equipped with 50 receive antennas and 50 transmit antennas. Other parameters are set as $\beta_L = \beta_E = \beta_J = 1$, $\sigma_I = 1$, $\gamma_{Jmax} = 15$ dB. The massive array jammer uses $\gamma_{Jmax} = 15$ dB as its jamming power. From the figure, we can observe that from the view-point of the illegitimate side, a massive array jammer have the worst performance. The legitimate side can easily counter the attack of the jammer by increasing its transmit power. A massive array eavesdropper shows a better performance than the jammer does when her can successfully wiretap the information from the legitimate side. However, when the transmit power at the legitimate side increases, no improvement is witnessed in the performance of the eavesdropper. The proposed cyber-weapon achieves the best performance among the three adversaries since her can dynamically launch different malicious attack scenarios.

Fig. 10 illustrates the effect of Eve's self-interference on the ergodic secrecy rate of the considered system in the perfect and imperfect channel estimation schemes. The system parameters are set as $M = 40$, $K = 100$, $N = 40$, $\beta_L = 10$, $\beta_E = \beta_J = 1$, and $\gamma_A = \gamma_J = 1$ dB. When the effect of self-interference increases, the ergodic secrecy rate of the considered system increases. Besides, it also reveals that the higher effect of self-interference leads to the smaller error of the imperfect channel estimation is. It can be explained that when the self-interference effect is high, the eavesdropping rate converges to zero. Therefore, the difference in the ergodic rates of the perfect channel estimation and imperfect channel estimation schemes is considered by the imperfect channel estimation of the jamming link.

VI. Conclusion

In this paper, from the perspective of the illegitimate side, the abilities of a full-duplex massive array cyber-weapon have been investigated with taking the effect of imperfect channel estimation at the cyber-weapon into consideration. The exact closed-form, tight approximation, and asymptotic expressions of the ergodic secrecy rate of the considered system in the

[7]The proposed optimization scheme uses the large-scale fading time scale which changes at least some 40 times slower than the small-scale fading (instantaneous channel gain) [29]. As a consequence, our proposed power allocation is done a few times per second, while the power allocation relying on the instantaneous channel gains must be done every some milliseconds.

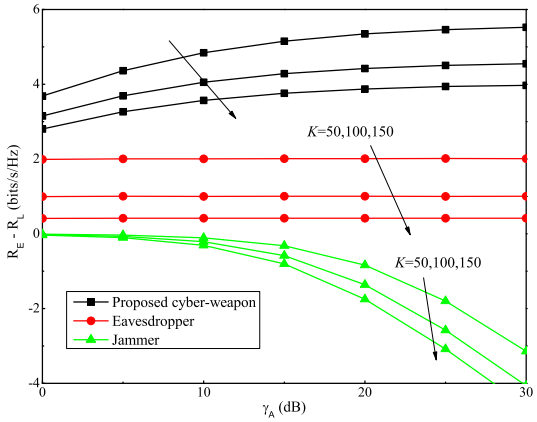

Fig. 9: Performance comparison of the proposed cyber-weapon with a massive array eavesdropper and a massive array jammer.

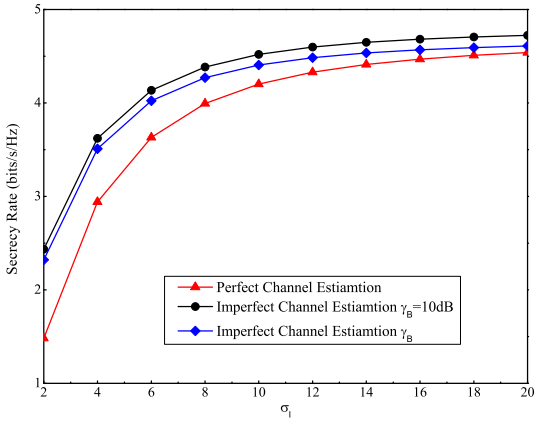

Fig. 10: Effect of the self-interference on the secrecy rate.

perfect and imperfect channel estimation schemes at the cyber-weapon have been derived. The results have revealed that under disadvantage conditions, i.e., imperfect channel estimation and the self-interference, the proposed cyber-weapon can effectively degrade the legitimate channels while successfully obtaining the confidential information. In addition, a transmit power optimization scheme at the cyber-weapon can help to eavesdrop confidential information even more efficiently. When the advanced technologies, i.e., full-duplex radio and massive array, are deployed by the illegitimate side, the legitimate side should apply protecting scenarios for the training phases as well as the information transmission phase.

Appendix A
Proof of Lemma 1 and Lemma 3

From (10), the ergodic rate of the legitimate channel is expressed as

$$R_{\mathsf{L}} = \mathbb{E}\left\{\log_2\left(1+\frac{\gamma_{\mathsf{A}}\left\|\boldsymbol{g}_{\mathsf{L}}\right\|^2}{\gamma_{\mathsf{J}}N\beta_{\mathsf{J}}+1}\right)\right\}. \tag{A.1}$$

From (1), it is observed that $\left\|\boldsymbol{g}_{\mathsf{L}}\right\|^2 = \beta_{\mathsf{L}}\left\|\boldsymbol{h}_{\mathsf{L}}\right\|^2$ in which $X = \left\|\boldsymbol{h}_{\mathsf{L}}\right\|^2$ follows the gamma distribution, i.e., $X \sim \Gamma(K,1)$. The probability density function (PDF) of X is $f_X(x) = \frac{1}{\Gamma(K)}x^{K-1}\exp(-x)$. Thus, the ergodic rate of the legitimate channel is derived as follows:

$$\begin{aligned}
R_{\mathsf{L}} &= \int_0^\infty \log_2\left(1+\frac{\gamma_{\mathsf{A}}\beta_{\mathsf{L}}}{\gamma_{\mathsf{J}}N\beta_{\mathsf{J}}}x\right) f_X(x)\,dx \\
&= \frac{1}{\Gamma(K)\ln 2}\int_0^\infty \ln\left(1+\frac{\gamma_{\mathsf{A}}\beta_{\mathsf{L}}}{\gamma_{\mathsf{J}}N\beta_{\mathsf{J}}}x\right)x^{K-1}\exp(-x)dx \\
&= \frac{1}{\ln 2}\sum_{k=0}^{K-1}\frac{1}{(K-1-k)!}\left(\frac{-\gamma_{\mathsf{J}}N\beta_{\mathsf{J}}-1}{\gamma_{\mathsf{A}}\beta_{\mathsf{L}}}\right)^{K-k-1} \\
&\times\left[-\exp\left(\frac{\gamma_{\mathsf{J}}N\beta_{\mathsf{J}}+1}{\gamma_{\mathsf{A}}\beta_{\mathsf{L}}}\right)\mathrm{Ei}\left(\frac{-\gamma_{\mathsf{J}}N\beta_{\mathsf{J}}-1}{\gamma_{\mathsf{A}}\beta_{\mathsf{L}}}\right)\right. \\
&+\left.\sum_{l=1}^{K-k-1}(l-1)!\left(\frac{-\gamma_{\mathsf{J}}N\beta_{\mathsf{J}}-1}{\gamma_{\mathsf{A}}\beta_{\mathsf{L}}}\right)^{-l}\right].
\end{aligned} \tag{A.2}$$

(A.2) is obtained with the help of [28, Eq. (4.337.5)]. Similarly, the exact closed-form for the ergodic rate of the eavesdropping is attained as in (16).

Appendix B
Proof of Lemma 5

When the transmit power of Alice is high, the asymptotic expression for the ergodic legitimate rate can be calculated as

$$\begin{aligned}
R_{\mathsf{S}}^{\mathsf{u,asym}} &= \left[\log_2\left(\lim_{\gamma_{\mathsf{A}}\to\infty}\Psi(\gamma_{\mathsf{J}})\right)\right]^+ \\
&= \left[\log_2\left(\frac{(\gamma_{\mathsf{J}}\sigma_{\mathsf{I}}^2+1)\beta_{\mathsf{L}}K}{(\gamma_{\mathsf{J}}N\beta_{\mathsf{J}}+1)M\beta_{\mathsf{E}}}\right)\right]^+.
\end{aligned} \tag{B.1}$$

Appendix C
Proof of Power Optimization Scheme at Eve

The first derivative of $\Theta(\gamma_{\mathsf{J}})$ is given as

$$\Theta'(\gamma_{\mathsf{J}}) = \frac{-ac\gamma_{\mathsf{J}}^2+2bc\gamma_{\mathsf{J}}+ae+bd}{(c\gamma_{\mathsf{J}}^2+d\gamma_{\mathsf{J}}+e)^2}. \tag{C.1}$$

From the condition $a\gamma_{\mathsf{J}}+b>0$, we consider three cases, i.e., $a\le 0$ and $b>0$, $a>0$ and $b\ge 0$, and $a>0$ and $b<0$.

1) Case 1— $a\le 0$ and $b>0$: in this case, it is observed that $\Theta(\gamma_{\mathsf{J}})$ is minimal when $\gamma_{\mathsf{J}}=0$. Therefore, the optimal solution for transmit power at Eve $\gamma_{\mathsf{J}}^*=0$.

2) Case 2— $a>0$ and $b\ge 0$: Considering the discriminant of quadratic equation $\Theta'(\gamma_{\mathsf{J}})=0$ as follows:

$$\Delta = 4b^2c^2+4a^2ce+4abcd. \tag{C.2}$$

If $\Delta\le 0$ then $\Theta'(\gamma_{\mathsf{J}})<0\ \forall\gamma_{\mathsf{J}}>0$. Therefore, $\Theta(\gamma_{\mathsf{J}})$ is a decreasing function $\forall\gamma_{\mathsf{J}}>0$. The optimal solution γ_{J}^* is $\gamma_{\mathsf{J}}^*=0$.

If $\Delta>0$, equation $\Theta'(\gamma_{\mathsf{J}})=0$ has two different roots

$$\gamma_{\mathsf{J}1}^* = \frac{2bc+\sqrt{\Delta}}{2ac}>0 \text{ and } \gamma_{\mathsf{J}2}^* = \frac{2bc-\sqrt{\Delta}}{2ac}. \tag{C.3}$$

We consider two sub-cases $2bc>\sqrt{\Delta}$ and $2bc<\sqrt{\Delta}$.

In the sub-case $2bc>\sqrt{\Delta}$, we can observe that $\gamma_{\mathsf{J}2}^*>0$. As a consequence, $\Theta(\gamma_{\mathsf{J}})$ is increasing with $\gamma_{\mathsf{J}2}^*\le\gamma_{\mathsf{J}}\le\gamma_{\mathsf{J}1}^*$

and decreasing with $\gamma_{\mathsf{J}} > \gamma_{\mathsf{J1}}^*$ and $0 < \gamma_{\mathsf{J}} < \gamma_{\mathsf{J2}}^*$. Therefore, the optimal solution γ_{J}^* is

$$\gamma_{\mathsf{J}}^* = \arg \max_{\gamma_{\mathsf{J}} \in \{0, \gamma_{\mathsf{Jmax}}, \gamma_{\mathsf{J1}}^*\}} \Theta(\gamma_{\mathsf{J}}). \tag{C.4}$$

In the sub-case $2bc < \sqrt{\Delta}$, it is observed that $\gamma_{\mathsf{J2}}^* < 0$. Therefore, $\Theta(\gamma_{\mathsf{J}})$ is increasing with $0 \leq \gamma_{\mathsf{J}} \leq \gamma_{\mathsf{J1}}^*$ and decreasing with $\gamma_{\mathsf{J1}}^* < \gamma_{\mathsf{J}}$. As a result, the optimal solution γ_{J}^* is

$$\gamma_{\mathsf{J}}^* = \arg \max_{\mathcal{P}_{\mathsf{J}} \in \{0, \gamma_{\mathsf{Jmax}}, \gamma_{\mathsf{J1}}^*\}} \Theta(\gamma_{\mathsf{J}}). \tag{C.5}$$

3) Case 3— $a > 0$ and $b < 0$: The condition for the transmit power of Eve becomes $\gamma_{\mathsf{J}} > \frac{-b}{a} > 0$. We assume that $\gamma_{\mathsf{Jmax}} > \frac{-b}{a}$. It is observed that $\Delta > 0$, $\gamma_{\mathsf{J1}}^* > 0$, and $\gamma_{\mathsf{J2}}^* < 0$. Therefore, $\Theta(\gamma_{\mathsf{J}})$ is increasing with $\frac{-b}{a} \leq \gamma_{\mathsf{J}} \leq \gamma_{\mathsf{J1}}^*$ and decreasing with $\gamma_{\mathsf{J}} > \gamma_{\mathsf{J1}}^*$. As a result, the optimal solution γ_{J}^* is

$$\gamma_{\mathsf{J}}^* = \min\left(\gamma_{\mathsf{J1}}^*, \gamma_{\mathsf{Jmax}}\right). \tag{C.6}$$

In the other cases, i.e., $a\gamma_{\mathsf{J}} + b < 0$, the ergodic eavesdropping rate is smaller than the ergodic legitimate rate , i.e., $R_{\mathsf{E}}^{\mathsf{l}} < R_{\mathsf{L}}^{\mathsf{u}}$. In these cases, the optimal transmit power of Eve is $\gamma_{\mathsf{J}}^* = 0$.

Appendix D
Proof of Lemma 8

From (35), it is observed that

$$\mathbb{E}\left\{\hat{\boldsymbol{g}}_{\mathsf{E}}\hat{\boldsymbol{g}}_{\mathsf{E}}^H\right\} = \left[\frac{\mathcal{P}_{\mathsf{A}}^2\beta_{\mathsf{E}}^3}{(\mathcal{P}_{\mathsf{A}}\beta_{\mathsf{E}} + \sigma_0^2)^2} + \frac{\mathcal{P}_{\mathsf{A}}\beta_{\mathsf{E}}^2\sigma_0^2}{(\mathcal{P}_{\mathsf{A}}\beta_{\mathsf{E}} + \sigma_0^2)^2}\right]\boldsymbol{I}_M. \tag{D.1}$$

Besides, we have that $\bar{\boldsymbol{g}}_{\mathsf{E}} \sim \sqrt{\beta_{\mathsf{E}}}\ \mathcal{CN}(0, \boldsymbol{I}_M)$. Therefore, $\hat{\boldsymbol{g}}_{\mathsf{E}} \sim \beta_{\mathsf{E}}\sqrt{\frac{\gamma_{\mathsf{A}}}{\gamma_{\mathsf{A}}\beta_{\mathsf{E}}+1}}\ \mathcal{CN}(0, \boldsymbol{I}_M)$. Consequently, $\left\|\hat{\boldsymbol{g}}_{\mathsf{E}}\right\|^2$ can be rewritten as $\left\|\hat{\boldsymbol{g}}_{\mathsf{E}}\right\|^2 = \frac{\gamma_{\mathsf{A}}\beta_{\mathsf{E}}^2}{1+\gamma_{\mathsf{A}}\beta_{\mathsf{E}}}Y$, where Y follows gamma distribution, i.e., $Y \sim \Gamma(M, 1)$. The PDF of Y is

$$f_Y(y) = \frac{1}{\Gamma(M)} y^{M-1}\exp(-y). \tag{D.2}$$

The exact closed-form of the ergodic eavesdropping rate when imperfect channel estimation is considered at Eve can be calculated as follows:

$$\begin{aligned}
R_{\mathsf{E}} &= \mathbb{E}\left\{\log_2\left(1 + \frac{\gamma_{\mathsf{A}}\left\|\hat{\boldsymbol{g}}_{\mathsf{E}}\right\|^2}{\frac{\gamma_{\mathsf{A}}\beta_{\mathsf{E}}}{\gamma_{\mathsf{A}}\beta_{\mathsf{E}}+1} + \gamma_{\mathsf{J}}\sigma_{\mathsf{I}}^2 + 1}\right)\right\} \\
&= \int_0^\infty \frac{1}{\Gamma(M)}\log_2\left(1 + \frac{\gamma_{\mathsf{A}}^2\beta_{\mathsf{E}}^2}{(\gamma_{\mathsf{A}}\beta_{\mathsf{E}}+1)(\gamma_{\mathsf{J}}\sigma_{\mathsf{I}}^2+1) + \gamma_{\mathsf{A}}\beta_{\mathsf{E}}}y\right) \\
&\times y^{M-1}\exp(-y)dy \\
&= \frac{1}{\ln 2}\sum_{m=0}^{M-1}\frac{1}{(M-m-1)!} \\
&\times \left(-\frac{(\gamma_{\mathsf{A}}\beta_{\mathsf{E}}+1)(\gamma_{\mathsf{J}}\sigma_{\mathsf{I}}^2+1) + \gamma_{\mathsf{A}}\beta_{\mathsf{E}}}{\gamma_{\mathsf{A}}^2\beta_{\mathsf{E}}^2}\right)^{M-m-1} \\
&\times \left[-\exp\left(\frac{(\gamma_{\mathsf{A}}\beta_{\mathsf{E}}+1)(\gamma_{\mathsf{J}}\sigma_{\mathsf{I}}^2+1) + \gamma_{\mathsf{A}}\beta_{\mathsf{E}}}{\gamma_{\mathsf{A}}^2\beta_{\mathsf{E}}^2}\right)\right. \\
&\times \mathrm{Ei}\left(-\frac{(\gamma_{\mathsf{A}}\beta_{\mathsf{E}}+1)(\gamma_{\mathsf{J}}\sigma_{\mathsf{I}}^2+1) + \gamma_{\mathsf{A}}\beta_{\mathsf{E}}}{\gamma_{\mathsf{A}}^2\beta_{\mathsf{E}}^2}\right) \\
&+ \left.\sum_{p=1}^{M-m-1}(p-1)!\left(-\frac{(\gamma_{\mathsf{A}}\beta_{\mathsf{E}}+1)(\gamma_{\mathsf{J}}\sigma_{\mathsf{I}}^2+1) + \gamma_{\mathsf{A}}\beta_{\mathsf{E}}}{\gamma_{\mathsf{A}}^2\beta_{\mathsf{E}}^2}\right)^{-p}\right].
\end{aligned} \tag{D.3}$$

(D.3) is obtained with the help of [28, Eq. (4.337.5)].

Appendix E
Analysis for the Case of Multi-Antenna Receiver

We use the channel capacity of the point-to-point Gaussian MIMO channel as an upper bound for the legitimate rate of the channel from Alice to Bob when multiple antennas are used at Bob. We assume the most optimistic scenario when the multi-antenna receiver can cancel all the interference from the jammer. Thus, the channel capacity of the point-to-point Gaussian MIMO channels with equal power allocation at the transmitter is given as [30], [31]

$$C_{\mathsf{L}} = \mathbb{E}\left\{\log_2\det\left(\boldsymbol{I}_{\mathsf{V}} + \left(\frac{\gamma_{\mathsf{A}}}{K}\right)\boldsymbol{H}\boldsymbol{H}^*\right)\right\}, \tag{E.1}$$

where $\det(\cdot)$ denotes the determinant, K and V are the numbers of antennas at Alice and Bob, respectively, $\boldsymbol{H}$ is the $V \times K$ channel matrix from Alice to Bob, elements of $\boldsymbol{H}$ are i.i.d. $\mathcal{CN}(0,1)$ random variables. For fixed V, $\frac{\boldsymbol{H}\boldsymbol{H}^*}{K} \to \boldsymbol{I}_{\mathsf{V}}$ almost surely when K goes to infinity. The capacity is re-written as

$$C_{\mathsf{L}} \to V\log_2(1+\gamma_{\mathsf{A}}). \tag{E.2}$$

From the above upper bound of the legitimate rate and (17), we have an upper bound for the secrecy rate of the considered system with multiple antennas at Bob as follows:

$$R_{\mathsf{S}} \to \left[\log_2\left(\frac{(1+\gamma_{\mathsf{A}})^V(\gamma_{\mathsf{J}}\sigma_{\mathsf{I}}^2+1)}{\gamma_{\mathsf{J}}\sigma_{\mathsf{I}}^2+1+\gamma_{\mathsf{A}}M\beta_{\mathsf{E}}}\right)\right]^+. \tag{E.3}$$

From (E.3), we can see that when the number of receive antennas at Eve is large, this secrecy rate upper bound still converges to zero.

APPENDIX F
ANALYSIS AND NUMERICAL RESULTS FOR THE CASE OF IMPERFECT CHANNEL ESTIMATION AT THE LEGITIMATE USERS

A. Channel Estimation at Alice

Bob sends training signals to Alice for enabling Alice creating the pre-code matrix. At Alice, the received signal is

$$\boldsymbol{y}_{\mathsf{A}} = \sqrt{\mathcal{P}_{\mathsf{B}}}\boldsymbol{g}_{\mathsf{L}} x_{sp} + \boldsymbol{w}_{\mathsf{A}}, \tag{F.1}$$

where $\boldsymbol{w}_{\mathsf{A}} \sim \sigma_0 \mathcal{CN}(0, \boldsymbol{I}_M)$ is the AWGN at Alice. In this work, we assume that MMSE channel estimation is processed at Alice. The estimated channel from Alice to Bob is given as

$$\hat{\boldsymbol{g}}_{\mathsf{L}} = \mathbb{C}_{\boldsymbol{g}_{\mathsf{L}},\boldsymbol{y}_{\mathsf{A}}} \mathbb{C}^{-1}_{\boldsymbol{y}_{\mathsf{A}},\boldsymbol{y}_{\mathsf{A}}} \boldsymbol{y}_{\mathsf{A}} = \frac{\mathcal{P}_{\mathsf{B}}\beta_{\mathsf{L}}}{\mathcal{P}_{\mathsf{B}}\beta_{\mathsf{L}} + \sigma_0^2}\boldsymbol{g}_{\mathsf{L}} + \frac{\sqrt{\mathcal{P}_{\mathsf{B}}}\beta_{\mathsf{L}}}{\mathcal{P}_{\mathsf{B}}\beta_{\mathsf{L}} + \sigma_0^2}\boldsymbol{w}_{\mathsf{A}} x_{sp}^*, \tag{F.2}$$

where $\mathbb{C}_{\hat{\boldsymbol{g}}_{\mathsf{L}},\boldsymbol{y}_{\mathsf{A}}} = \sqrt{\mathcal{P}_{\mathsf{B}}}\beta_{\mathsf{L}}\boldsymbol{I}_M x_{sp}^*$, $\mathbb{C}_{\boldsymbol{y}_{\mathsf{A}},\boldsymbol{y}_{\mathsf{A}}} = (\mathcal{P}_{\mathsf{B}}\beta_{\mathsf{L}} + \sigma_0^2)\boldsymbol{I}_M$. From (F.2), it is observed that $\hat{\boldsymbol{g}}_{\mathsf{L}} \sim \mathcal{CN}(0, \sigma_{\mathsf{A}}^2 \boldsymbol{I}_N)$, $\gamma_{\mathsf{B}} = \frac{\mathcal{P}_{\mathsf{B}}}{\sigma_0^2}$, and $\sigma_{\mathsf{A}} = \beta_{\mathsf{L}}\sqrt{\frac{\gamma_{\mathsf{B}}}{\gamma_{\mathsf{B}}\beta_{\mathsf{L}}+1}}$.

We denote the estimation error for the jamming channel as follows:

$$\boldsymbol{\mathcal{E}}_{\mathsf{A}} \triangleq \boldsymbol{g}_{\mathsf{L}} - \hat{\boldsymbol{g}}_{\mathsf{L}} = \frac{\sigma_0^2}{\mathcal{P}_{\mathsf{B}}\beta_{\mathsf{L}} + \sigma_0^2}\boldsymbol{g}_{\mathsf{L}} - \frac{\sqrt{\mathcal{P}_{\mathsf{B}}}\beta_{\mathsf{L}}}{\mathcal{P}_{\mathsf{B}}\beta_{\mathsf{L}} + \sigma_0^2} w_{\mathsf{A}} x_{sp}^*, \tag{F.3}$$

where $\boldsymbol{\mathcal{E}}_{\mathsf{A}}$ is independent of $\hat{\boldsymbol{g}}_{\mathsf{L}}$ and $\boldsymbol{\mathcal{E}}_{\mathsf{A}} \sim \mathcal{CN}(0, (\beta_{\mathsf{L}} - \sigma_{\mathsf{A}}^2)\boldsymbol{I}_M)$.

B. Channel Estimation at Bob

After estimating the channel from Bob to Alice, Alice sends pilot back to Bob. The purpose is to provide Bob CSI for decoding the signals. The received signal at Bob is

$$y_{\mathsf{B}} = \sqrt{\mathcal{P}_{\mathsf{A}}}\boldsymbol{g}_{\mathsf{L}}^H \frac{\hat{\boldsymbol{g}}_{\mathsf{L}}}{\|\hat{\boldsymbol{g}}_{\mathsf{L}}\|} x_{\mathsf{sp}} + w_{\mathsf{B}} = \sqrt{\mathcal{P}_{\mathsf{A}}} c_{\mathsf{B}} x_{\mathsf{sp}} + w_{\mathsf{B}}, \tag{F.4}$$

where $c_{\mathsf{B}} = \boldsymbol{g}_{\mathsf{L}}^H \frac{\hat{\boldsymbol{g}}_{\mathsf{L}}}{\|\hat{\boldsymbol{g}}_{\mathsf{L}}\|}$. We have $\mathbb{E}\{c_{\mathsf{B}}\} = \sigma_{\mathsf{A}} \frac{\Gamma\left(\frac{2K+1}{2}\right)}{\Gamma(K)}$ and $\mathbb{E}\left\{|c_{\mathsf{B}}|^2\right\} = (K-1)\sigma_{\mathsf{A}}^2 + \beta_{\mathsf{L}}$.

Bob performs MMSE to estimate c_{B},

$$\begin{aligned}\hat{c}_{\mathsf{B}} &= \mathbb{E}\{c_{\mathsf{B}}\} + \mathbb{C}_{c_{\mathsf{B}},y_{\mathsf{B}}} \mathbb{C}^{-1}_{y_{\mathsf{B}},y_{\mathsf{B}}} (y_{\mathsf{B}} - \mathbb{E}\{y_{\mathsf{B}}\}) \\ &= \frac{\mathcal{P}_{\mathsf{A}} \mathbb{V}\mathrm{ar}(c_{\mathsf{B}}) c_{\mathsf{B}} + \sqrt{\mathcal{P}_{\mathsf{A}}} \mathbb{V}\mathrm{ar}(c_{\mathsf{B}}) w_{\mathsf{B}} + \sigma_0^2 \mathbb{E}\{c_{\mathsf{B}}\}}{\mathcal{P}_{\mathsf{A}} \mathbb{V}\mathrm{ar}(c_{\mathsf{B}}) + \sigma_0^2},\end{aligned} \tag{F.5}$$

where $\mathbb{C}_{c_{\mathsf{B}},y_{\mathsf{B}}} = \sqrt{\mathcal{P}_{\mathsf{A}}}(\mathbb{E}\left\{|c_{\mathsf{B}}|^2\right\} - (\mathbb{E}\{c_{\mathsf{B}}\})^2) = \sqrt{\mathcal{P}_{\mathsf{A}}}\,\mathbb{V}\mathrm{ar}(c_{\mathsf{B}})$ and $\mathbb{C}_{y_{\mathsf{B}},y_{\mathsf{B}}} = \mathcal{P}_{\mathsf{A}}(\mathbb{E}\left\{|c_{\mathsf{B}}|^2\right\} - (\mathbb{E}\{c_{\mathsf{B}}\})^2) + \sigma_0^2 = \mathcal{P}_{\mathsf{A}}\,\mathbb{V}\mathrm{ar}(c_{\mathsf{B}}) + \sigma_0^2$. We also have $\mathbb{E}\{\hat{c}_{\mathsf{B}}\} = \frac{\gamma_{\mathsf{A}}\,\mathbb{V}\mathrm{ar}(c_{\mathsf{B}})}{\gamma_{\mathsf{A}}\,\mathbb{V}\mathrm{ar}(c_{\mathsf{B}})+1}\mathbb{E}\{c_{\mathsf{B}}\}$ and $\mathbb{E}\left\{|\hat{c}_{\mathsf{B}}|^2\right\} = \frac{\gamma_{\mathsf{A}}\,\mathbb{V}\mathrm{ar}(c_{\mathsf{B}})}{(\gamma_{\mathsf{A}}\,\mathbb{V}\mathrm{ar}(c_{\mathsf{B}})+1)^2}\left(\gamma_{\mathsf{A}}\,\mathbb{V}\mathrm{ar}(c_{\mathsf{B}})\mathbb{E}\left\{|c_{\mathsf{B}}|^2\right\} + (\mathbb{E}\{c_{\mathsf{B}}\})^2 + \mathbb{V}\mathrm{ar}(c_{\mathsf{B}})\right)$.

The estimation error is

$$\mathcal{E}_{\mathsf{B}} = c_{\mathsf{B}} - \hat{c}_{\mathsf{B}} = \frac{\sigma_0^2 c_{\mathsf{B}} - \sqrt{\mathcal{P}_{\mathsf{A}}}\,\mathbb{V}\mathrm{ar}(c_{\mathsf{B}}) w_{\mathsf{B}} - \sigma_0^2 \mathbb{E}\{c_{\mathsf{B}}\}}{\mathcal{P}_{\mathsf{A}}\,\mathbb{V}\mathrm{ar}(c_{\mathsf{B}}) + \sigma_0^2}. \tag{F.6}$$

We have $\mathbb{E}\{\mathcal{E}_{\mathsf{B}}\} = \frac{\mathbb{E}\{c_{\mathsf{B}}\}}{\gamma_{\mathsf{A}}\,\mathbb{V}\mathrm{ar}(c_{\mathsf{B}})+1}$, $\mathbb{E}\left\{|\mathcal{E}_{\mathsf{B}}|^2\right\} = \frac{\mathbb{E}\left\{|c_{\mathsf{B}}|^2\right\} + (\mathbb{E}\{c_{\mathsf{B}}\})^2 + \gamma_{\mathsf{A}}[\mathbb{V}\mathrm{ar}(c_{\mathsf{B}})]^2}{(\gamma_{\mathsf{A}}\,\mathbb{V}\mathrm{ar}(c_{\mathsf{B}})+1)^2}$, and $\mathbb{V}\mathrm{ar}(\mathcal{E}_{\mathsf{B}}) = \frac{\mathbb{E}\left\{|c_{\mathsf{B}}|^2\right\} + \gamma_{\mathsf{A}}[\mathbb{V}\mathrm{ar}(c_{\mathsf{B}})]^2}{(\gamma_{\mathsf{A}}\,\mathbb{V}\mathrm{ar}(c_{\mathsf{B}})+1)^2}$.

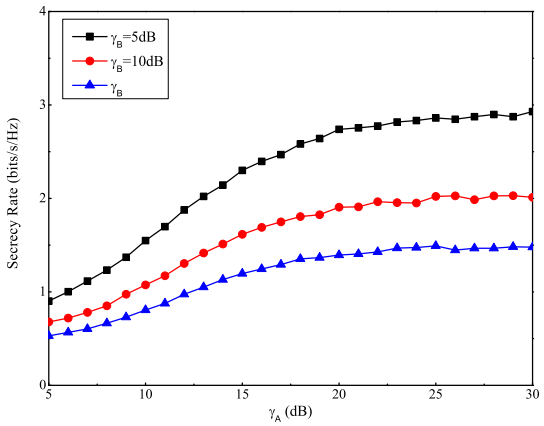

Fig. 11: Secrecy rate with imperfect CSI at the legitimate users

C. Legitimate Rate

The received signal at Bob in information transmission phase is

$$y_{\mathsf{B}} = \sqrt{\mathcal{P}_{\mathsf{A}}} c_{\mathsf{B}} x + \sqrt{\mathcal{P}_{\mathsf{J}}}\,\|\hat{\boldsymbol{g}}_{\mathsf{J}}\|\, x_{\mathsf{J}} + \sqrt{\mathcal{P}_{\mathsf{J}}}\boldsymbol{\mathcal{E}}_{\mathsf{J}}^H \frac{\hat{\boldsymbol{g}}_{\mathsf{J}}}{\|\hat{\boldsymbol{g}}_{\mathsf{J}}\|} x_{\mathsf{J}} + w_{\mathsf{B}}. \tag{F.7}$$

Since Bob only knows the estimated effective channel $\hat{c}_{\mathsf{B}}$, the ergodic legitimate rate is given in (F.8) on the top of the next page. It is observed that the ergodic legitimate rate in this case is lower than that of the case in which perfect channel estimation is considered at the legitimate users. The ergodic illegitimate rate can be calculated similarly to (46).

D. Numerical Results

Fig. 11 shows the simulation results of the considered system's secrecy rate in the case of imperfect channel estimation is considered at the legitimate users. In this setup, $K = M = N = 50$, $\beta_{\mathsf{L}} = 10$, $\beta_{\mathsf{E}} = 1$, $\beta_{\mathsf{J}} = 0.1$, $\sigma_{\mathsf{I}} = 10$, $\gamma_{\mathsf{J}} = 10$ dB, $\gamma_{\mathsf{B}} = \{5, 10, 15\}$ dB. It is observed that when the transmit power at Alice increases, the secrecy rate increases and then saturates. This phenomenon is similar to the phenomenon in Fig. 3 and Fig. 4. Besides, Fig. 11 also demonstrates the effect of transmit power at Bob. Decreasing the transmit power at Bob makes the channel estimation process at Eve more difficult and removes the advantage of multiple jamming antennas at Eve, followed by an increase in the secrecy rate. This point has been discussed in Remark 4.

REFERENCES

[1] E. Larsson, O. Edfors, F. Tufvesson, and T. Marzetta, "Massive MIMO for next generation wireless systems," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 186–195, Feb. 2014.

[2] D. W. K. Ng, E. S. Lo, and R. Schober, "Energy-efficient resource allocation in OFDMA systems with large numbers of base station antennas," *IEEE Trans. Wireless Commun.*, vol. 11, no. 9, pp. 3292–3304, Sep. 2012.

[3] H. V. Poor, "Information and inference in the wireless physical layer," *IEEE Commun. Mag.*, pp. 40–47, Feb. 2012.

[4] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: State of the art and beyond," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 32–39, Dec. 2015.

$$
\begin{aligned}
R_{\mathsf{L}} &= \mathbb{E}\left\{\log_2\left(1+\frac{\left|\mathbb{E}\left\{\sqrt{\mathcal{P}_{\mathsf{A}}}c_{\mathsf{B}}\middle|\hat{c}_{\mathsf{B}}\right\}\right|^2}{\mathcal{P}_{\mathsf{A}}\,\mathbb{V}\mathrm{ar}(c_{\mathsf{B}}|\hat{c}_{\mathsf{B}})+\mathbb{E}\left\{\left|\sqrt{\mathcal{P}_{\mathsf{J}}}\left\|\hat{\boldsymbol{g}}_{\mathsf{J}}\right\|x_{\mathsf{J}}+\sqrt{\mathcal{P}_{\mathsf{J}}}\boldsymbol{\mathcal{E}}_{\mathsf{J}}^H\frac{\hat{\boldsymbol{g}}_{\mathsf{J}}}{\|\hat{\boldsymbol{g}}_{\mathsf{J}}\|}x_{\mathsf{J}}+w_{\mathsf{B}}\right|^2\middle|\hat{c}_{\mathsf{B}}\right\}}\right)\right\}\\
&\approx \mathbb{E}\left\{\log_2\left(1+\frac{\mathcal{P}_{\mathsf{A}}|\hat{c}_{\mathsf{B}}|^2}{\mathcal{P}_{\mathsf{A}}\,\mathbb{V}\mathrm{ar}(\mathcal{E}_{\mathsf{B}})+\mathcal{P}_{\mathsf{J}}\mathbb{E}\left\{\|\hat{\boldsymbol{g}}_{\mathsf{J}}\|^2\right\}+\mathcal{P}_{\mathsf{J}}\mathbb{E}\left\{\left|\boldsymbol{\mathcal{E}}_{\mathsf{J}}^H\frac{\hat{\boldsymbol{g}}_{\mathsf{J}}}{\|\hat{\boldsymbol{g}}_{\mathsf{J}}\|}\right|^2\right\}+\sigma_0^2}\right)\right\}\\
&= \mathbb{E}\left\{\log_2\left(1+\frac{\gamma_{\mathsf{A}}|\hat{c}_{\mathsf{B}}|^2}{\gamma_{\mathsf{A}}\,\mathbb{V}\mathrm{ar}(\mathcal{E}_{\mathsf{B}})+\frac{\gamma_{\mathsf{J}}\gamma_{\mathsf{B}}\beta_{\mathsf{J}}^2N}{\gamma_{\mathsf{B}}\beta_{\mathsf{J}}+1}+\frac{\gamma_{\mathsf{J}}\beta_{\mathsf{J}}}{\gamma_{\mathsf{B}}\beta_{\mathsf{J}}+1}+1}\right)\right\}. \qquad \text{(F.8)}
\end{aligned}
$$

[5] L. Wang, K. J. Kim, T. Q. Duong, M. Elkashlan, and H. V. Poor, "Security enhancement of cooperative single carrier systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 1, pp. 90–103, Jan. 2015.

[6] N.-P. Nguyen, T. Q. Duong, H. Q. Ngo, Z. Hadzi-Velkov, and L. Shu, "Secure 5G wireless communications: A joint relay selection and wireless power transfer approach," *IEEE Access*, vol. 4, pp. 3349–3359, June 2016.

[7] N.-P. Nguyen, C. Kundu, H. Q. Ngo, T. Q. Duong, and B. Canberk, "Secure full-duplex small-cell networks in a spectrum sharing environment," *IEEE Access*, vol. 4, pp. 3087–3099, June 2016.

[8] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766–4781, Sep. 2014.

[9] X. Chen, J. Chen, and T. Liu, "Secure transmission in wireless powered massive MIMO relaying systems: Performance analysis and optimization," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8025–8035, Oct. 2016.

[10] B. Chen, C. Zhu, L. Shu, M. Su, J. Wei, V. C. M. Leung, and J. J. P. C. Rodrigues, "Securing uplink transmission for lightweight single-antenna UEs in the presence of a massive MIMO eavesdropper," *IEEE Access*, vol. 4, pp. 5374–5384, Sep. 2016.

[11] J. Zhu and W. Xu, "Securing massive MIMO via power scaling," *IEEE Commun. Lett.*, vol. 20, no. 5, pp. 1014–1017, May 2016.

[12] J. Zhu, R. Schober, and V. K. Bhargava, "Linear precoding of data and artificial noise in secure massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2245–2261, Mar. 2016.

[13] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[14] T. T. Do, H. Q. Ngo, T. Q. Duong, T. J. Oechtering, and M. Skoglund, "Massive MIMO pilot retransmission strategies for robustification against jamming," *IEEE Commun. Lett.*, pp. 1–1, 2016.

[15] G. T. Amariucai and S. Wei, "Half-duplex active eavesdropping in fast-fading channels: A block-Markov Wyner secrecy encoding scheme," *IEEE Trans. Inf. Theory*, vol. 58, no. 7, pp. 4660–4677, Jul. 2012.

[16] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission with an active eavesdropper," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3880–3900, Jul. 2016.

[17] M. Karlsson and E. G. Larsson, "Massive MIMO as a cyber-weapon," in *Proc. Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, Nov. 2014, pp. 661–665.

[18] A. El Shafie, K. Tourki, Z. Ding, and N. Al-Dhahir, "Probabilistic jamming/eavesdropping attacks to confuse a buffer-aided transmitter-receiver pair," *IEEE Commun. Lett.*, pp. 1–1, 2017.

[19] Y. Deng, K. J. Kim, T. Q. Duong, M. Elkashlan, G. K. Karagiannidis, and A. Nallanathan, "Full-duplex spectrum sharing in cooperative single carrier systems," *IEEE Trans. Cognit. Commun. Netw.*, vol. 4, no. 1, pp. 68–82, June 2016.

[20] A. Mukherjee and A. L. Swindlehurst, "A full-duplex active eavesdropper in MIMO wiretap channels: Construction and countermeasures," in *Proc. Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, Nov. 2011, pp. 265–269.

[21] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 2012.

[22] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via jamming for rate maximization over rayleigh fading channels," *IEEE Commun. Lett.*, vol. 5, no. 1, pp. 80–83, Feb. 2016.

[23] X. Tang, P. Ren, Y. Wang, and Z. Han, "Combating full-duplex active eavesdropper: a hierarchical game perspective," *IEEE Trans. Commun.*, vol. 65, no. 3, pp. 1379–1395, Mar. 2017.

[24] Q. Xiong, Y.-C. Liang, K. H. Li, and Y. Gong, "An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 932–940, May 2015.

[25] H. Q. Ngo, E. G. Larsson, and T. L. Marzetta, "Energy and spectral efficiency of very large multiuser MIMO systems," *IEEE Trans. Commun.*, vol. 61, no. 4, pp. 1436–1449, Apr. 2013.

[26] Hien Quoc Ngo, E. G. Larsson, and T. L. Marzetta, "Massive MU-MIMO downlink TDD systems with linear precoding and downlink pilots," in *Proc. Allerton Conference on Communication, Control, and Computing*, Monticello, IL, Oct. 2013, pp. 293–298.

[27] S. K. Mohammed and E. G. Larsson, "Single-user beamforming in large-scale miso systems with per-antenna constant-envelope constraints: The doughnut channel," *IEEE Trans. Wireless Commun.*, vol. 11, no. 11, pp. 3992–4005, Nov. 2012.

[28] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*, 7th ed. San Diego, CA: Academic press, 2007.

[29] T. S. Rappaport, *Wireless communications: principles and practice*. Upper Saddle River: Prentice-Hall, 1956.

[30] I. E. Telatar, "Capacity of multi-antenna gaussian channels," *Europ. Trans. Telecommu.*, vol. 10, pp. 585–595, Nov./Dec. 1999.

[31] G. J. Foschini, "Layered space-time architecture for wireless communication in a fading environment when using multi-element antennas," *Bell Labs Tech. J.*, vol. 1, no. 2, pp. 41–59, 1996.

Nam-Phong Nguyen (S'16) was born in Hanoi, Vietnam. He received the B.S. degree in electronics and telecommunication engineering and the M.S. degree in electronics engineering from the Hanoi University of Science and Technology, Vietnam, in 2012 and 2014, respectively. He is currently pursuing the Ph.D. degree with Queens University Belfast. His research interests include physical layer security, cognitive relay networks, energy harvesting communications, and massive MIMO.

Hien Quoc Ngo received the B.S. degree in electrical engineering from the Ho Chi Minh City University of Technology, Vietnam, in 2007, the M.S. degree in electronics and radio engineering from Kyung Hee University, South Korea, in 2010, and the Ph.D. degree in communication systems from Linköping University (LiU), Sweden, in 2015. In 2014, he visited the Nokia Bell Labs, Murray Hill, New Jersey, USA. From January 2016 to April 2017, Hien Quoc Ngo was a VR researcher at the Department of Electrical Engineering (ISY), LiU. He was also a Visiting Research Fellow at the School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, UK, funded by the Swedish Research Council.

Hien Quoc Ngo is currently a Lecturer at Queen's University Belfast, UK. His main research interests include massive (large-scale) MIMO systems, cell-free massive MIMO, physical layer security, and cooperative communications. He has co-authored many research papers in wireless communications and co-authored the Cambridge University Press textbook *Fundamentals of Massive MIMO* (2016).

Dr. Hien Quoc Ngo received the IEEE ComSoc Stephen O. Rice Prize in Communications Theory in 2015 and the IEEE Communications Society Leonard G. Abraham Prize in 2017. He also received the IEEE Sweden VT-COM-IT Joint Chapter Best Student Journal Paper Award in 2015. He was an *IEEE Communications Letters* exemplary reviewer for 2014, an *IEEE Transactions on Communications* exemplary reviewer for 2015, and an *IEEE Wireless Communications Letters* exemplary reviewer for 2016. He was a Guest Editor of IET Communications, special issue on "Recent Advances on 5G Communications" and a Guest Editor of IEEE Access, special issue on "Modelling, Analysis, and Design of 5G Ultra-Dense Networks", in 2017. He has been a member of Technical Program Committees for several IEEE conferences such as ICC, Globecom, WCNC, VTC, WCSP, ISWCS, ATC, ComManTel.

Trung Q. Duong (S'05, M'12, SM'13) received his Ph.D. degree in Telecommunications Systems from Blekinge Institute of Technology (BTH), Sweden in 2012. Since 2013, he has joined Queen's University Belfast, UK as a Lecturer (Assistant Professor). His current research interests include small-cell networks, ultra-dense networks, physical layer security, energy-harvesting communications, massive MIMO. He is the author or co-author of more than 270 technical papers published in scientific journals (145 articles) and presented at international conferences (125 papers).

Dr. Duong currently serves as an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON COMMUNICATIONS, IET COMMUNICATIONS, and a Senior Editor for IEEE COMMUNICATIONS LETTERS. He was awarded the Best Paper Award at the IEEE Vehicular Technology Conference (VTC-Spring) in 2013, IEEE International Conference on Communications (ICC) 2014, and IEEE Global Communications Conference (GLOBECOM) 2016. He is the recipient of prestigious Royal Academy of Engineering Research Fellowship (2016-2021).

Hoang Duong Tuan received the Diploma (Hons.) and Ph.D. degrees in applied mathematics from Odessa State University, Ukraine, in 1987 and 1991, respectively. He spent nine academic years in Japan as an Assistant Professor in the Department of Electronic-Mechanical Engineering, Nagoya University, from 1994 to 1999, and then as an Associate Professor in the Department of Electrical and Computer Engineering, Toyota Technological Institute, Nagoya, from 1999 to 2003. He was a Professor with the School of Electrical Engineering and Telecommunications, University of New South Wales, from 2003 to 2011. He is currently a Professor with the Centre for Health Technologies, University of Technology Sydney. He has been involved in research with the areas of optimization, control, signal processing, wireless communication, and biomedical engineering for more than 20 years.

Daniel Benevides da Costa (S'04-M'08-SM'14) was born in Fortaleza, Ceará, Brazil, in 1981. He received the B.Sc. degree in Telecommunications from the Military Institute of Engineering (IME), Rio de Janeiro, Brazil, in 2003, and the M.Sc. and Ph.D. degrees in Electrical Engineering, Area: Telecommunications, from the University of Campinas, SP, Brazil, in 2006 and 2008, respectively. His Ph.D thesis was awarded the Best Ph.D. Thesis in Electrical Engineering by the Brazilian Ministry of Education (CAPES) at the 2009 CAPES Thesis Contest. From 2008 to 2009, he was a Postdoctoral Research Fellow with INRS-EMT, University of Quebec, Montreal, QC, Canada. Since 2010, he has been with the Federal University of Ceará, where he is currently an Assistant Professor. Prof. da Costa is currently Editor of the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, IEEE ACCESS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, EURASIP JOURNAL ON WIRELESS COMMUNICATIONS AND NETWORKING, and KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS. He has also served as Associate Technical Editor of the IEEE COMMUNICATIONS MAGAZINE. From 2012 to 2017, he was Editor of the IEEE COMMUNICATIONS LETTERS. He has served as Guest Editor of several Journal Special Issues. He has been involved on the organization of several conferences. He is currently the Latin American Chapters Coordinator of the IEEE Vehicular Technology Society. Also, he acts as a Scientific Consultant of the National Council of Scientific and Technological Development (CNPq), Brazil and he is a Productivity Research Fellow of CNPq. From 2012 to 2017, he was Member of the Advisory Board of the Cear Council of Scientific and Technological Development (FUNCAP), Area: Telecommunications. Prof. da Costa is the recipient of three conference paper awards. He received the Exemplary Reviewer Certificate of the IEEE WIRELESS COMMUNICATIONS LETTERS in 2013, the Exemplary Reviewer Certificate of the IEEE COMMUNICATIONS LETTERS in 2016, the Certificate of Appreciation of Top Associate Editor for outstanding contributions to IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY in 2013, 2015 and 2016, and the Exemplary Editor Award of IEEE COMMUNICATIONS LETTERS in 2016. He is Distinguished Lecturer of the IEEE Vehicular Technology Society. He is a Senior Member of IEEE, Member of IEEE Communications Society and IEEE Vehicular Technology Society.